ASA Research

# Information Security

J. Carlton Collins
ASA Research - Atlanta, Georgia
770.734.0950
Carlton@ASAResearch.com

# Table of Contents

# Information Security for CPAs
# Course Information

| | |
|---|---|
| **Learning Objectives** | To make CPAs aware of the multitude of security threats and to provide solutions for minimizing and mitigating those threats. |
| **Course Level** | All levels |
| **Pre-Requisites** | None |
| **Advanced Preparation** | None |
| **Presentation Method** | Live lecture using full color projection systems and live Internet access with follow up course materials |
| **Recommended CPE Credit** | 8 hours |
| **Handouts** | Checklists, Web Links, Manual |
| **Instructors** | J. Carlton Collins, CPA |

*AdvisorCPE is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be addressed to the national Registry of CPE Sponsors, 150 Fourth Avenue, Nashville, TN, 37219-2417. Phone: 615.880.4200.*



**Contact Information:**
**J. Carlton Collins**
CARLTON@ASARESEARCH.COM
**770.734.0950**

# WEB SITES MAINTAINED BY INSTRUCTOR:

| | |
|---|---|
| Main Web Site | www.ASAResearch.com |
| Mirrored Web Site | www.AccountingSoftwareAdvisor.com |
| Accounting Software Advice Web Site | www.AccountingSoftwareAnswers.com |
| Top Accounting Software Consultants | www.AccountingSoftwareConsulting.com |
| Accounting Software News Web Site | www.AccountingSoftwareNews.com |
| Accounting Software Feature Reports | www.AccountingSoftwareReports.com |
| CPE Information Web Site | www.AdvisorCPE.com |
| Hot List | www.CarltonCollins/footer/hotlist.htm |
| Miscellaneous and Example Web Site | www.CarltonCollins.com |
| Technology Advice Web Site | www.CPAAdvisor.us |
| Microsoft Excel Web Site | www.ExcelAdvisor.net |
| QuickBooks Web Site | www.QuickbooksAdvisor.info |
| Microsoft Accounting Systems Web Site | www.MBSAdvisor.com |
| Microsoft SBA Web Site | www.SBAAdvisor.com |
| Microsoft Office Web Site | www.OfficeAdvisor.us |

We publish all of our materials on the web as a service to the CPA community. Please feel free to learn about our other topics at these great web sites. Thank you.

# Locks

## Chapter 1

## Locks

Virtually all computers, files, and data are protected behind locked doors, locked cabinets, or locked files – but how secure are those locks? It turns out that most locks today are not very secure at all. Not only can most locks be picked by professional locksmiths, but hundreds of YouTube clips teach novice people how to pick locks as well. As examples, consider these YouTube clips and web sites:

| | |
|---|---|
| Open any padlock with a beer can - | http://www.metacafe.com/watch/yt-1eGxRQlWTrM/open_a_master_padlock_with_a_beer_can/ |
| Learn how locks work | http://www.metacafe.com/watch/yt-cuLC9klMsRI/the_visual_guide_to_lock_picking_part_06_of_10/ |
| Open door locks with picking tools | http://www.metacafe.com/watch/877739/kwikset_door_lock_picked/ |
| Make your own pick tools | http://www.metacafe.com/watch/1029493/home_made_lock_picks/ |
| Pick a padlock with homemade pick tools | http://www.metacafe.com/watch/1015152/how_to_open_padlock_lockpicking/ |
| Open door locks with a bump hammer | http://www.metacafe.com/watch/yt-zTfEwChCG0U/brockhage_bump_hammer_set/ |
| Open a door lock with a pick gun | http://www.metacafe.com/watch/884219/how_to_pick_locks_with_a_lock_pick_gun_lockpicking_tutorial/ |
| Open a car with a tennis ball | http://www.metacafe.com/watch/410981/blondie_unlocks_car/ |
| Open car with wood wedge and pole | http://www.metacafe.com/watch/1078391/how_to_unlock_car_without_keys/ |
| Open a tubular lock | http://www.metacafe.com/watch/1029502/lock_picking_tubular_locks/ |
| Pick a club and pick a car ignition | http://www.metacafe.com/watch/1029496/lock_picking_club_and_car_ignition/ |
| Pick tools described | http://www.metacafe.com/watch/1363050/lock_picking_with_all_my_sets_tools/ |
| Order picking tools online | http://www.lockpicks.com/index.asp?PageAction=VIEWCATS&Category=204 |
| Order a pick gun online | http://www.lockpicks.com/index.asp?PageAction=VIEWCATS&Category=215 |
| Order a bump hammer online | http://www.lockpicks.com/index.asp?PageAction=VIEWCATS&Category=324 |
| Order car pick tools online | |

# Government Compliance

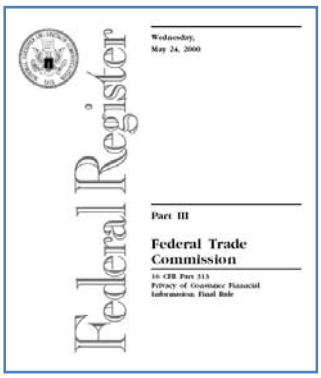
## Federally Required Security Measures

# Chapter 2

# Gramm-Leach-Bliley Act

http://www.ftc.gov/os/2000/05/65fr33645.pdf

http://www.keytlaw.com/Links/glbact.htm




The Gramm-Leach-Bliley Act has been deemed to apply to CPA firms, and nearly all financial institutions. Within this Act, the Safeguards Rule of GLB requires CPAs and financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. Then plan went into effect as of March 2001. This plan must include:

1. Assign at least one employee to manage the safeguards.
2. Constructing a thorough [risk management] on each department handling the nonpublic information.
3. Develop, monitor, and test a program to secure the information. and
4. Change the safeguards as needed with the changes in how information is collected, stored, and used.

***Do you have a Written Plan?***

# HIPPA Security Requirements

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services (HHS) to establish national standards for the security of electronic health care information. The Act limits the ways that health plans, pharmacies, hospitals and other covered entities can use patients' personal medical information as follows: (For more detail see http://www.castlemans.org/HIPPA/Fact%20Sheet1.htm)

1. Access to Medical Records (Patients can see their own records and correct errors)
2. Notice of Privacy Practices (Patients must be provided notice of privacy measures)
3. Limits on Use of Personal Medical Information (Only minimal information can be shared)
4. Prohibition on Marketing (Patient information cannot be used in marketing)
5. Stronger State Laws (State laws are not trumped)
6. Confidential communications (Communications must be confidential)
7. Complaints (http://www.hhs.gov/ocr/hipaa/ or by calling (866) 627-7748)
8. Written Privacy Procedures (Now required and must be detailed)
9. Employee Training and Privacy Officer (Both are now required)
10. Public Responsibilities (Disclosures of health must be made in a responsible manner)
11. Equivalency Requirements (Private and government hospitals must both comply)
12. Penalties (Up to $250,000 and 10 years in prison)

## Sarbanes Oxley Compliance

The Sarbanes-Oxley Act of 2002 (SOX) created new business rules regarding the storage and management of corporate financial data. SOX holds many publicly held companies and all Registered Public Accounting Firms to a rigorous set of standards. These rules set guidelines for how data should be stored, accessed, and retrieved.

| Section Number | Description of Rule |
|---|---|
| **Section 103:** Auditing, Quality Control, And Independence Standards And Rules | The Board shall: (1) register public accounting firms; (2) establish, or adopt, by rule, "auditing, quality control, ethics, independence, and other standards relating to the preparation of audit reports for issuers;" The Board requires registered public accounting firms to "prepare, and maintain for a period of not less than 7 years, audit work papers, and other information related to any audit report, in sufficient detail to support the conclusions reached in such report." |
| **Section 104:** Inspections of Registered Public Accounting Firms | Quality inspections must be conducted annually for firms auditing more than 100 issues per year, or every 3 years for all other firms. The SEC or the Board may order impromptu inspections of any firm at any time. |
| **Section 105(d):** Investigations And Disciplinary Proceedings; Reporting of Sanctions | All documents prepared or received by the Board are regarded "confidential and privileged as an evidentiary matter (and shall not be subject to civil discovery or other legal process) in any proceeding in any Federal or State court or administrative agency, unless and until presented in connection with a public proceeding or [otherwise] released" in connection with a disciplinary action. |
| **Title VIII:** Corporate & Criminal Fraud Accountability Act of 2002 | "Knowingly" destroying or creating documents to "impede, obstruct or influence" any federal investigation, whether it exists or is contemplated, is a felony. |
| **Section 802:** Mandatory Document Retention | This section instructs auditors to maintain "all audit or review work papers" for five years from the end of the fiscal period during which the audit or review was concluded. It also directs the Securities and Exchange Commission (SEC) to disseminate any necessary rules and regulations relating to the retention of relevant records from an audit or review. This section makes it unlawful knowingly and willfully to violate these new provisions - including any rules and regulations disseminated by the SEC - and imposes fines, a maximum term of 10 years' imprisonment or both. |
| **Section 802:** Document Alteration or Destruction<br><br>**Section 1102:** Tampering With a Record or Otherwise Impeding an Official Proceeding | This section criminalizes knowingly altering, destroying, mutilating, or concealing any document with the intent to impair the object's integrity or availability for use in an official proceeding or to otherwise obstruct, influence or impede any official proceeding. |

# Securing Hard Drives & Laptops

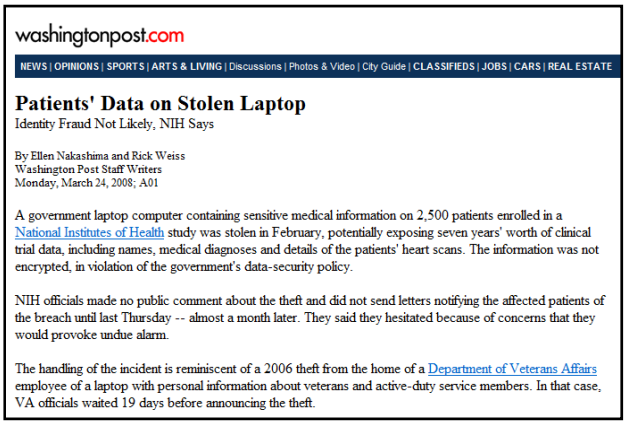
## Chapter 3

# Stolen Laptops

Laptop computers are key targets for thieves, and these thieves are not after the laptop for the value of the computer – it is the value on the data and embedded passwords that entice these thieves. Laptops are easy targets. They are small and easy to grab, and once stolen they blend in without attracting attention. In 2008, the Government Accountability Office found that at least 19 of 24 agencies reviewed had experienced at least one breach that could expose people's personal information to identity theft. The Computer Security Institute/FBI Computer Crime & Security Survey found the average theft of a laptop to cost a company $89,000.

Many laptops contain data which can be exploited or resold on the black market to unscrupulous people. In particular, embedded passwords can allow hackers to access critical systems and personal information that can be used to perpetuate identity theft and other crimes. Presented below is a sampling of some laptop thefts that have been reported in the news in the past few years. A lengthy list of breaches via stolen laptops and hacks can be seen here: [http://www.privacyrights.org/ar/ChronDataBreaches.htm](http://www.privacyrights.org/ar/ChronDataBreaches.htm).

**Organization:** National Institute of Health
**Date of Theft:** February 2008
**Type of Data Stolen:** Patient data for 2,500 patients over a 7 year period
**How Stolen:** From an employee's home



washingtonpost.com

NEWS | OPINIONS | SPORTS | ARTS & LIVING | Discussions | Photos & Video | City Guide | CLASSIFIEDS | JOBS | CARS | REAL ESTATE

**Patients' Data on Stolen Laptop**

Identity Fraud Not Likely, NIH Says

By Ellen Nakashima and Rick Weiss
Washington Post Staff Writers
Monday, March 24, 2008; A01

A government laptop computer containing sensitive medical information on 2,500 patients enrolled in a National Institutes of Health study was stolen in February, potentially exposing seven years' worth of clinical trial data, including names, medical diagnoses and details of the patients' heart scans. The information was not encrypted, in violation of the government's data-security policy.

NIH officials made no public comment about the theft and did not send letters notifying the affected patients of the breach until last Thursday -- almost a month later. They said they hesitated because of concerns that they would provoke undue alarm.

The handling of the incident is reminiscent of a 2006 theft from the home of a Department of Veterans Affairs employee of a laptop with personal information about veterans and active-duty service members. In that case, VA officials waited 19 days before announcing the theft.

**Nashville laptop theft may cost $1 million**

**With Social Security numbers at risk, county officials offer registered voters in Tennessee county a year of free identity theft protection at the cost $10 per account**

By Robert McMillan, IDG News Service
January 14, 2008

Talkback | E-mail | Printer Friendly | Reprints | Text Size A A

The theft of a laptop containing Social Security numbers of Nashville, Tenn.-area voters is expected to cost local officials about $1 million as they roll out identity-theft protection to those affected.

Free IT resource

Download the Windows Server(R) 2008 Beta: Join the global community.

Sponsored by Microsoft

Video

To your page volumes be true

Sponsored by HP

Related Stories

How to make the (new) iPhone work at work

Spam King trial set to start next month

230 retailers affected by data breach after tape lost

County officials say that thieves broke into Davidson County Election Commission offices on the weekend before Christmas, smashing a window with a rock and then making off with a $3,000 router, a digital camera, and a pair of Dell Latitude laptops containing names and Social Security numbers of all 337,000 registered voters in the county.

County election officials began notifying residents of the breach on Jan. 2, and the local government is offering victims one year of free identity theft protection from Debix Identity Protection Network.

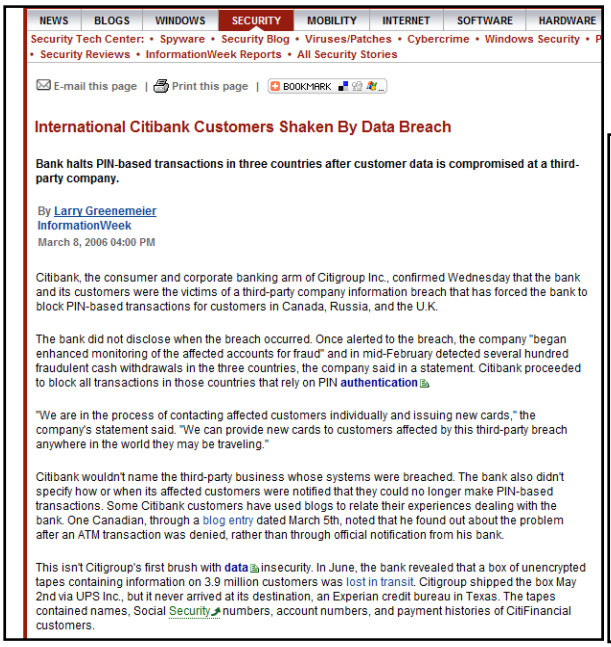
Debix says that 25 to 35 percent of victims of this type of breach typically request this service. With the city paying Debix just under $10 per account, the price tag for the laptop theft is expected to be in the $1 million range.

Since state data breach disclosure laws went into effect a few years ago, the theft of an unencrypted laptop computer can become a major problem for any organization that stores sensitive data.

"It is a very bad information-handling practice to keep sensitive information about individuals including their Social Security numbers on an unencrypted laptop or any other device that is removable," said Paul Stephens director of policy and advocacy with Privacy Rights Clearinghouse, a privacy advocacy group that has tracked the exposure of 217 million records in the United States over the past three years.

**Organization:** Davidson County Election Commission - (Nashville, TN)
**Date of Theft:** December 28, 2007
**Type of Data Stolen:** Names and complete Social Security numbers for 337,000 registered voters
**How Stolen:** Someone broke into several county offices over Christmas and stole laptop computers

**Organization:** Citibank Student Loan Corporation
**Date of Theft:** March 8, 2006
**Type of Data Stolen:** Information on 3.9 million customers
**How Stolen:** Lost in transit while being shipped



NEWS | BLOGS | WINDOWS | SECURITY | MOBILITY | INTERNET | SOFTWARE | HARDWARE

Security Tech Center: • Spyware • Security Blog • Viruses/Patches • Cybercrime • Windows Security • P
• Security Reviews • InformationWeek Reports • All Security Stories

E-mail this page | Print this page | BOOKMARK

**International Citibank Customers Shaken By Data Breach**

**Bank halts PIN-based transactions in three countries after customer data is compromised at a third-party company.**

By Larry Greenemeier
InformationWeek
March 8, 2006 04:00 PM

Citibank, the consumer and corporate banking arm of Citigroup Inc., confirmed Wednesday that the bank and its customers were the victims of a third-party company information breach that has forced the bank to block PIN-based transactions for customers in Canada, Russia, and the U.K.

The bank did not disclose when the breach occurred. Once alerted to the breach, the company "began enhanced monitoring of the affected accounts for fraud" and in mid-February detected several hundred fraudulent cash withdrawals in the three countries, the company said in a statement. Citibank proceeded to block all transactions in those countries that rely on PIN authentication.

"We are in the process of contacting affected customers individually and issuing new cards," the company's statement said. "We can provide new cards to customers affected by this third-party breach anywhere in the world they may be traveling."

Citibank wouldn't name the third-party business whose systems were breached. The bank also didn't specify how or when its affected customers were notified that they could no longer make PIN-based transactions. Some Citibank customers have used blogs to relate their experiences dealing with the bank. One Canadian, through a blog entry dated March 5th, noted that he found out about the problem after an ATM transaction was denied, rather than through official notification from his bank.

This isn't Citigroup's first brush with data insecurity. In June, the bank revealed that a box of unencrypted tapes containing information on 3.9 million customers was lost in transit. Citigroup shipped the box May 2nd via UPS Inc., but it never arrived at its destination, an Experian credit bureau in Texas. The tapes contained names, Social Security numbers, account numbers, and payment histories of CitiFinancial customers.

NEWS | POLITICS | OPINIONS | LOCAL | SPORTS | ARTS & LIVING | CITY GUIDE

SEARCH: go washingtonpost.com Web: Results by Google

washingtonpost.com > Technology > Tech Policy

TechNews.com

Print This Article
E-Mail This Article

QUICK QUOTES
Enter Symbol go
Tables | Portfolio | Index

MOST VIEWED ARTICLES
Technology | On the Site
Updated 4:17 p.m. ET
• Patients' Data on Stolen Laptop
• New Google Search Tool Finds Web Publishers' Concerns
• Sony Retracts Bloatware

E-MAIL NEWSLETTERS
View a Sample and Sign Up
• TechNews Daily Report
• Personal Finance
• Personal Tech

**Computer Theft Puts Floridians At Risk**
Government Laptop Has Sensitive Data

*By Christopher Lee and Del Quentin Wilber*
Washington Post Staff Writers
Thursday, August 10, 2006; Page A06

A laptop computer from the inspector general's office at the Department of Transportation was stolen last month, putting the sensitive personal information of nearly 133,000 Florida residents at risk, acting Inspector General Todd J. Zinser said yesterday.

The laptop, assigned to a special agent in the Miami office, was stolen from a government vehicle on July 27 in Doral, Fla., Zinser told Florida Gov. Jeb Bush (R) yesterday in a letter.

The computer, which requires a password to operate, contains the unencrypted names, Social Security numbers, birth dates and addresses of 42,792 Florida residents who hold a pilot's license; 80,667 people in the Miami-Dade

WHO'S BLOGGING?
Read what bloggers are saying about this article.
• Liberal Values - Defending Liberty and Enlightened Thought
• Tech Law Prof Blog
• BelchSpeak

**Organization:** Transportation Security Administration (TSA)
**Date of Theft:** August 10, 2006
**Type of Data Stolen:** Social Security numbers, payroll information, and bank account data for approximately 133,000 employee records
**How Stolen:** From a government vehicle

**Organization:** Internal Revenue Service (IRS)
**Date of Theft:** June, 2006
**Type of Data Stolen:** 291 employees and job applicants, including fingerprints, names, Social Security numbers, and dates of birth
**How Stolen:** In transit on an airline flight


msnbc

Technology & science / Security

Lost IRS laptop stored employee fingerprints

Hundreds notified they are at risk of ID theft, including some applicants

By Bob Sullivan
Technology correspondent
MSNBC
updated 4:46 p.m. ET, Mon., June. 5, 2006

MSNBC A laptop computer containing fingerprints of Internal Revenue Service employees is missing, MSNBC.com has learned.

Bob Sullivan
Technology correspondent
• Profile
• E-mail

The computer was lost during transit on an airline flight in the western United States, IRS spokesman Terry Lemon said. No taxpayer information was on the lost laptop, Lemon said.

In all, the IRS believes the computer contained information on 291 employees and job applicants, including fingerprints, names, Social Security numbers, and dates of birth. The


LOCAL SPORTS ARTS & LIVING CITY GUIDE

washingtonpost.com Web: Results by Google

echnology

SECURITY FIX

BRIAN KREBS

Brian Krebs on Computer Security

About This Blog | Archives | RSS Feed (What's RSS?)

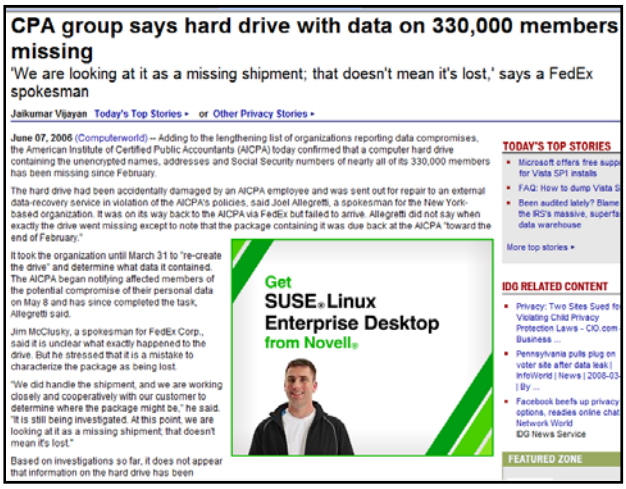
FTC Laptop Theft Exposes Consumer Data

The **Federal Trade Commission** -- an agency whose mission includes consumer protection and occasionally involves suing companies for negligence in protecting customer information -- today disclosed a recent theft of two laptop computers containing personal and financial data on consumers.

In a statement, the FTC said two employee laptops were stolen from a locked vehicle. The PCs contained data on about 110 people that was "gathered in law enforcement investigations and included, variously, names, addresses, Social Security numbers, dates of birth, and in some instances, financial account numbers."

**Organization:** Federal Trade Commission (FTC)
**Date of Theft:** June 22, 2006
**Type of Data Stolen:** Data on about 110 people that was "gathered in law enforcement investigations"
**How Stolen:** Stolen from a locked vehicle

**Organization:** American Institute of Certified Public Accountants (AICPA)
**Date of Theft: June,** 2006
**Type of Data Stolen:** Unencrypted hard drive containing names, addresses and Social Security numbers of 330,000 AICPA members.
**How Stolen:** Lost during shipping



**CPA group says hard drive with data on 330,000 members missing**

'We are looking at it as a missing shipment; that doesn't mean it's lost,' says a FedEx spokesman

Jaikumar Vijayan Today's Top Stories ▸ or Other Privacy Stories ▸

June 07, 2006 (Computerworld) -- Adding to the lengthening list of organizations reporting data compromises, the American Institute of Certified Public Accountants (AICPA) today confirmed that a computer hard drive containing the unencrypted names, addresses and Social Security numbers of nearly all of its 330,000 members has been missing since February.

The hard drive had been accidentally damaged by an AICPA employee and was sent out for repair to an external data-recovery service in violation of the AICPA's policies, said Joel Allegretti, a spokesman for the New York-based organization. It was on its way back to the AICPA via FedEx but failed to arrive. Allegretti did not say when exactly the drive went missing except to note that the package containing it was due back at the AICPA "toward the end of February."

It took the organization until March 31 to "re-create the drive" and determine what data it contained. The AICPA began notifying affected members of the potential compromise of their personal data on May 8 and has since completed the task, Allegretti said.

Jim McClusky, a spokesman for FedEx Corp., said it is unclear what exactly happened to the drive. But he stressed that it is a mistake to characterize the package as being lost.

"We did handle the shipment, and we are working closely and cooperatively with our customer to determine where the package might be," he said. "It is still being investigated. At this point, we are looking at it as a missing shipment; that doesn't mean it's lost."

Based on investigations so far, it does not appear that information on the hard drive has been

TODAY'S TOP STORIES

- Microsoft offers free supp for Vista SP1 installs
- FAQ: How to dump Vista S
- Been audited lately? Blame the IRS's massive, superfa data warehouse

More top stories ▸



IDG RELATED CONTENT

- Privacy: Two Sites Sued fo Violating Child Privacy Protection Laws - CIO.com Business ...
- Pennsylvania pulls plug on voter site after data leak | InfoWorld | News | 2008-03 | By ...
- Facebook beefs up privacy options, readies online chat Network World
IDG News Service

FEATURED ZONE

ELECTRONIC PRIVACY INFORMATION CENTER

**Veterans Affairs Data Theft**

Latest News

- **Stolen Veterans Affairs Laptop and Hard Drive Are Found.** The stolen laptop computer and hard drive containing sensitive data for up to 26.5 million veterans, their spouses, and active-duty military personnel have been found, according to Veterans Affairs Secretary Jim Nicholson. This comes as newly discovered documents show that Veterans Affairs had given permission in 2002 for the analyst, from whom the equipment was stolen, to work from home with data that included millions of Social Security numbers, disability ratings and other personal information. Agency officials previously said the analyst was fired because he violated agency procedure by taking the data home. (Jun. 29)
- **Scope of Veterans Affairs Data Theft Widens.** The personal information of about 1.1 million active-duty military personnel, 430,000 members of the National Guard and 645,000 members of the Reserves, was stolen in the recent theft of computer data from the Department of Veterans Affairs, the agency announced Tuesday. The agency previously said (pdf) that all 26.5 million people affected by the data theft were veterans and their spouses. The data include Social Security numbers and disability ratings. Privacy Rights Clearinghouse offers ID theft prevention tips. (Jun. 7)
- **Department of Veterans Affairs Reports Massive Data Theft.** The Department of Veterans Affairs announced today that an agency employee took home records on 26.5 million veterans that were subsequently stolen by a burglar. The data included names, Social Security numbers, and dates of birth, as well as some disability ratings. The FBI and the VA Inspector General's Office have launched "full-scale investigations." Information for those who are concerned about identity theft is available from the Federal Trade Commission. (May 22)

Background

An information security breach by a Veterans Affairs employee resulted in the theft from his Maryland home of unencrypted data affecting 26.5 million people. The agency has estimated that it will cost between $100 million to $500 million to prevent and cover possible losses from the data theft. Though the theft occurred on May 3, 2006, the agency waited until May 22 to inform those who were affected. The delay was just one of many failures by Veterans Affairs in this incident.

**Organization:** US Government Veterans Affairs Administration
**Date of Theft:** May 3, 2006
**Type of Data Stolen:** 26.5 million veterans, their spouses, and active-duty military personnel
**How Stolen:** Laptop stolen from employees home

The list of security breaches due to laptop thefts seems endless, here are ten more:

1. A laptop that belonged to an Ernst & Young employee was stolen from a vehicle. The computer contained personal information of 243,000 Hotels.com customers.

ERNST & YOUNG
*Quality In Everything We Do*

hotels.com
WE KNOW HOTELS INSIDE AND OUT.™

2. American International Group, a major insurance company, became responsible for private data of 970,000 potential customers when their file server and several laptop computers were stolen from its Midwest offices.


3. An Equifax Inc., company laptop was stolen from a travelling employee. Information compromised included employee names and Social Security numbers.


4. 13,000 District of Columbia employees and retirees were put in danger of identity theft when a laptop belonging ING U.S. Financial Services was stolen from an employee's home.


5. A laptop containing debit card information and Social Security numbers of 65,000 persons was stolen from YMCA's seemingly safe administrative offices.


6. Four laptop computers containing names, Social Security numbers, and addresses of 72,000 customers were stolen from the Medicaid insurance provider Buckeye Community Health Plan.


7. A Boeing employee's laptop was grabbed at an airport, compromising 3,600 employees Social Security numbers, addresses and phone numbers. Again in 2006 Boeing lost an unencrypted computer hard drive which held the names and Social Security numbers of approximately 382,000 workers and former employees, including addresses, phone numbers, birth dates and salary information.


8. Stolen UC Berkeley laptop exposed personal data of nearly 100,000.


9. A laptop computer stolen from an MCI employee's automobile in 2005 included the names and social security numbers of 16,500 MCI employees.


10. In 2006 Fidelity Investments reported the theft of a laptop computer's hard drive which contained personal information for approximately 196,000 HP employees.


These types of events raise many security concerns for the information contained on these computers could be used by criminals to assume other's identities and abscond with their cash and assets. The distressing part is that all of these events could have been minimized if only the computer's owners had taken a few minutes to set up a password encrypting the computer's contents. While setting up a computer BIOS password or a Windows Logon password will thwart a novice thief, these measures are is not enough because thieves can simply remove the hard drive and install it in a different computer (which uses a different operating system) as a secondary drive which then enables the criminal to view the data on the stolen device. To fully protect the system, you must encrypt the entire hard drive. For example, Microsoft Vista includes a solution called BitLocker which once setup, automatically encrypts the contents of entire hard drive. Similar solutions are offered by PGP, Guardian Edge, and TruCrypt.

# Measures you Can Take to Protect Your Laptop Computer

1. **Physical Security** - Physical devices can be used to secure your laptop computer, ranging from chains and alarms to ID programs which clearly identify the computer as belonging to you.

   a. ***Cables*** - Targus and Kensington both manufacture cable devices that physically secure your laptop by locking it to a table or other object. These cables are very tough, but they can be cut with power tools or large clippers. While these products can be circumvented, they are good for deterring crimes of opportunity.




   b. ***Alarms -*** Motion sensing locking devices are also available, and these add an extra layer of security by setting off a loud alarm if the cable is tampered with or if the device goes out of range by a certain distance.


   c. ***Fingerprint Security*** - Biometrics devices such as a the fingerprint readers which are included in all IBM laptops or available from Microsoft encrypt your passwords and associate them with your fingerprint. In the future, you register your fingerprint and the appropriate password is then entered for you.


   Fingerprints can be hacked, it is not as hard as you might think. You can use a gummy bear to pick up a print and then apply it to the fingerprint reader.

Of course you can also make a fingerprint using super glue as was demonstrated in both Hollywood movies Beverly Hills Cops and National Treasure.



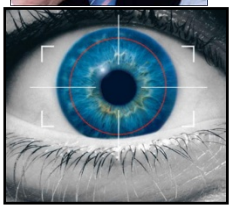
The Crypto-Gram Newsletter was the first to publicize the Gummy Bear Hack as follows:

A Japanese cryptographer has demonstrated how fingerprint recognition devices can be fooled using a combination of low cunning, cheap kitchen supplies and a digital camera. First Tsutomu Matsumoto used gelatin (as found in Gummy Bears and other sweets) and a plastic mould to create a fake finger, which he found fooled fingerprint detectors four times out of five. Flushed with his success, he took latent fingerprints from a glass, which he enhanced with a cyanoacrylate adhesive (super-glue fumes) and photographed with a digital camera. Using PhotoShop, he improved the contrast of the image and printed the fingerprint onto a transparency sheet. Here comes the clever bit.

Matsumoto took a photo-sensitive printed-circuit board (which can be found in many electronic hobby shops) and used the fingerprint transparency to etch the fingerprint into the copper. From this he made a gelatin finger using the print on the PCB, using the same process as before. Again this fooled fingerprint detectors about 80 per cent of the time.

d. ***Retina Scanners*** – Similar to fingerprint technology discussed above, retina scan products are also available, for example the Qritek mouse (pictured below and to the right) is priced at $315 has a built-in retina scanner.




If your laptop did not come with a biometric security device built in, you will need to purchase a third-party add on that connects through the USB or PC card ports. Because these devices must function via the operating system,

they can be easily bypassed. They are most useful for securing data when combined with encryption software, but biometric devices are viewed as more of a password enhancement than an additional layer of security for your laptop. While biometric devices are cool, they provide little additional benefit over simply using passwords and encryption to protect your property.

**2. Laptop Identification Programs**

a. ***Manufacturer's Program -*** If your laptop is stolen, you will have a much better chance of eventually getting it back if you registered the device with the manufacturer. If the device is registered, when you report it as stolen, many manufacturers can track the serial number of the device if and when it is logged onto the Internet (in some cases); and if the laptop is subsequently brought in for repairs, a record will exist. You should keep track of your laptop's serial number, even if you do not register it.

b. ***The STOP Program -*** You can also enroll your laptop into the STOP Program. In this case an identification tag provides proof of ownership and perhaps acts as a deterrent to theft. Laptops protected with STOP plates are registered in a Web-based database which increases the chances of the safe return of lost, stolen, or misplaced laptops, notebooks and other equipment.

STOP® Security Tracking of Office Property

c. ***Personalize Your Laptop*** - Personalizing your laptop can make it much more likely for you to get it back in the event of theft. By engraving identification information into the device itself, or by using a permanent marker, you provide yourself with some very tangible descriptive information which you can provide to police. You can also use Toshiba's LapJacks – material which sticks firmly to the laptop cover, but can also be removed cleanly if required. Similarly, Pixel Decal sells skins for $20. For those with money to burn, NVousPC (pronounced "envious PC") makes custom notebooks with a personalized paint job - customers work with graphic designers to customize every panel — not just the cover.

d. ***Laptop Tracing Software*** - To increase the odds of having your laptop returned, consider using a laptop tracing software solution. These products work by stealthily sending out signals on the Internet. When your laptop is stolen, simply report the theft to the maker of the tracing software and when the laptop's new owner connects to the Internet, the company can provide tracking information to the police. Some tracking software also provides the

ability to delete selected data once the laptop has been reported as stolen. Most of these software packages are difficult to detect and remove, and some claim to be able to survive re-partitioning and reformatting of the hard drive. If the hard drive is removed, so is the tracing software. Most of these services work on a yearly subscription basis. Popular tracking software packages are as follows:

i. ETrace
ii. Computrace
iii. GadgetTrak for Windows PC
iv. The CyberAngel w/ Wi-Trac by CyberAngel Security Solutions, Inc.
v. BackStopp by Virtuity, Ltd.
vi. XTool Laptop Tracker by XTool Mobile Security, Inc.
vii. LoJack for laptops.
viii. PC PhoneHome by Brigadoon Software, Inc.
ix. nTracker by SyNet Electronics, Inc.
x. Inspice Trace by Inspice.
xi. Verey Mac Theft Recovery Software
xii. DataDots

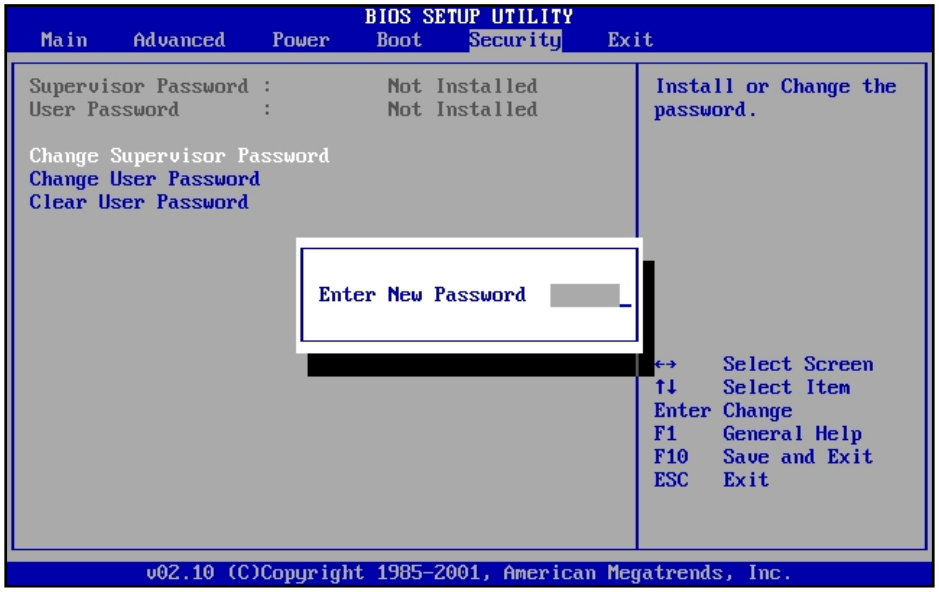
3. **Common Sense Measures** – Watch your laptop closely at the airport – many thieves target this venue and use decoys in order to steal laptop computers. They know it will take you some time to travel to your destination before you can close down password protected web sites. Don't leave your laptop visible in your car, your trunk, your hotel room, or anywhere while traveling. Consider using a plain carrying case or backpack to carry your laptop, as this can deter would be thieves.

4. **Data Encryption** - It is extremely hard, if not impossible, to effectively secure a computer to which an intruder has physical access. There are four steps you can take to make it rather frustratingly hard and time consuming for the bad guys to get at your vital data however, as follows:

   a. **BIOS Password Protection** - Most computers can be password protected by setting a password in the BIOS (Basic Input/Output System) built into the motherboard of the computer. On desktop computers, password protecting the BIOS is a poor security measure because a thief can simply open up the case and use a jumper to reset the CMOS, or remove the battery for a few minutes to erase the password. It's a different story with a laptop however. Laptop computers are built on proprietary designs, using motherboards created specifically for each model. It is often not possible to get at the CMOS battery of a laptop without special tools and know-how, or at least not without destroying the machine in the process. Generally speaking, if you want to reset the BIOS password on a laptop, you will need to ship it back to the manufacturer, something your average thief is going to be understandably reluctant to do.

   This makes BIOS password protection a rather good option for users who are concerned about the possibility of data theft, as a BIOS password makes it impossible to boot into any operating system until it is answered. It's not foolproof, as many manufacturers have built 'backdoor' keystroke combinations into their systems which can bypass even BIOS passwords, but it's a great start. To set the BIOS password, press the DEL key several times immediately after the POST screen comes up (some manufacturers use a different key stroke, but this should be indicated on your screen during boot-

up, or in the manual) to enter the BIOS setup. You are looking for 'set password' or something similar. Set it (write it down so you don't forget it) and save and exit. The next time you boot, you will be prompted for a password after POST. Make sure you keep a record of the password.




b. **Use Strong Passwords** - After stealing your laptop, a thief has an unlimited time in which to crack your passwords. They will likely attempt to use the SAM and SYSTEM file password hash extraction method in combination with some sort of password cracking software to discover your password. Let's assume that your password is “happy”' It would take them about 5 minutes or less to crack using a fast computer. If the password were happy44 add another 10 minutes maybe… But what if your password was (hAP5py28) You've just extended the time it will take them to crack your password to several hours, perhaps days. The more numbers, uppercase letters, symbols and digits in your password, the harder it is to discover. Microsoft recommends using no less than 6-digit passwords with at least three of the following: lower case, uppercase, numbers and special characters. I would recommend using 16 digit passwords with a mixture of letters, characters and numbers. To make it easier for you, you might always use the same beginning or ending for all of your passwords such as an old phone number you remember, followed by a strong password (ie: 9126388947happy7755).

Also, changing the 'administrator' account to an alternate name is also a good measure to make it harder to break in. Everyone knows that Windows XP uses an administrator account, and that it cannot be disabled, so it is the prime target for data thieves. By renaming it 'Carlton' or something stranger still, you can add some time and frustration to your thief's life. To accomplish this:

1. Log into windows using an account that has administrative privileges (any user created during install process or the administrator account itself)
2. Right click on 'my computer' and select 'manage.'
3. From the computer management window, Expand 'local users and groups' then open the 'users' folder and highlight the 'administrator' account.

4. Right click and select 'rename' to change it.

c. **Encrypt Your Hard Drive (or Data Folder) –** There are a multitude of utilities out there that will easily boot your computer into an alternate OS like Linux and then reset your user passwords. It is also quite simple to grab a portable operating system that boots itself from CD (such as Knoppix), or a DOS boot disk with an NTFS reader on it and then copy the information straight off your laptop's drive. For that matter, laptop hard disks are generally easy to remove anyway. A thief could purchase an adaptor or a USB case and hook your laptop's hard drive up to his or her own system and siphon off your files.

Windows XP Professional, like Windows 2000 before it, features built in strong file encryption based on the identity of the user. When you use the Encrypting File System (EFS), a file is encrypted with an algorithm derived from the unique SID (System Identifier) number generated for each user account. Once the file is encrypted, it cannot be decrypted except by the original user (and anyone he chooses to grant access to the file). This means that any other user account will not be able to view the file, period. The encryption is permanent and remains on the file even when Windows is not running. It doesn't matter if a new account with the exact same name and password is created, only the original account with the original SID number can decrypt and read the file.

The benefits of using file encryption should be obvious. The only feasible way to break it without a supercomputer is to bypass it by gaining access to the user account that did the encrypting. If you set strong passwords this is very tough to do. None of the conventional methods of getting at secured data will work on encrypted files. Of course, encryption carries its own set of dangers. If the original user account is destroyed due to a system failure or user error, you too will lose all access to the encrypted data. It is possible (and highly recommended) to create a 'recovery agent' which provides a secondary account with the ability to recover the data. This can be created as a digital certificate which can be exported to a floppy disk, then applied to a user account when needed.

a. **How to encrypt files and folders in Windows XP** - (Note that you must be using the NTFS file system in order to use encryption.)

   1. Right click on the file or folder and select 'properties.'
   2. In the 'attributes' section at the bottom, click 'advanced.'


Check the 'encrypt contents to secure data' box, then click OK twice. In the case of a file, you will be prompted to choose between encrypting just that single file or the whole folder, and in the case of a folder, whether you wish to also encrypt any subfolders it may contain.

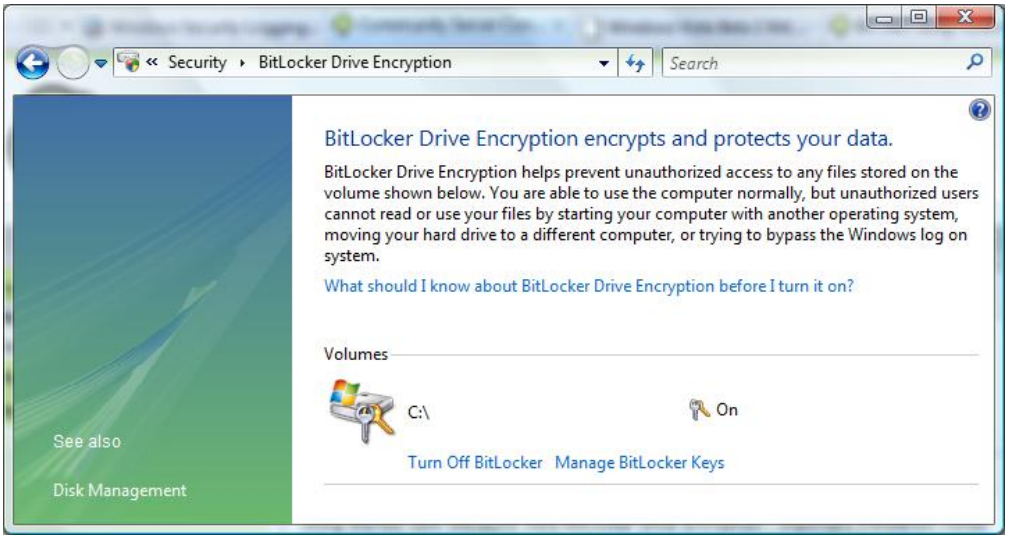
Creating a recovery agent:

1. Decide which user you wish to use as a data-recovery agent. It is recommended that you use the built in 'administrator' account.
2. Login as this account.
3. Go to 'start\run' and type 'cmd' to bring up the command prompt.
4. Type 'cipher /r:(pick a filename) to create a digital certificate for a recovery agent. You will be prompted to set a password. This creates two files in the 'my documents' folder of the current user. Be aware that these files can be used by anyone to become a data-recovery agent, so it is wise to remove them after we are finished this procedure.

b. **Windows Vista BitLocker** – BitLocker Drive Encryption is an integral new security feature in the Windows Vista operating system that ensures that data remains encrypted even if the computer is tampered with when the operating system is not running. This helps protect against attacks made by disabling or circumventing the installed operating system, or made by physically removing the hard drive to attack the data separately. BitLocker protects your data from theft or unauthorized viewing by encrypting the entire Windows volume. Microsoft Vista's BitLocker tool encrypts everything written to a BitLocker-protected volume, including the operating system, the registry, the hibernation and paging files, applications, and data used by applications, but not the boot sector, any bad sectors, or the volume metadata. BitLocker is transparent to the user,

and the user logon process is unchanged. However, if the TPM is missing or changed, or if the startup information has changed, BitLocker will enter recovery mode, and you will need a recovery password to regain access to the data.

BitLocker is designed for systems that have a compatible TPM microchip and BIOS. For more information about TPM specifications, visit the TPM Specifications section of the Trusted Computing Group's Web site (http://go.microsoft.com/fwlink/?LinkId=72757).




c. **TrueCrypt** – TrueCrypt is free open-source disk encryption software for Windows Vista/XP, Mac OS X, and Linux . The software creates a virtual encrypted disk within a file and mounts it as a real disk. It encrypts an entire partition or storage device such as USB flash drive or hard drive. It also encrypts a partition or drive where Windows is installed (pre-boot authentication). The encryption is automatic, real-time (on-the-fly) and transparent. Two levels of plausible deniability is provided as follows, in case an adversary forces you to reveal the password:


1) Hidden volume (steganography) - It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you

to solve such situations without revealing the password to your volume. The principle is that a TrueCrypt volume is created within another TrueCrypt volume (within the free space on the volume). Even when the outer volume is mounted, it is impossible to prove whether there is a hidden volume within it or not, because free space on any TrueCrypt volume is always filled with random data when the volume is created* and no part of the (dismounted) hidden volume can be distinguished from random data. Note that TrueCrypt does *not* modify the file system (information about free space, etc.) within the outer volume in any way.

The password for the hidden volume must be different from the password for the outer volume. To the outer volume, (before creating the hidden volume within it) you should copy some sensitive-looking files that you actually do NOT want to hide. These files will be there for anyone who would force you to hand over the password. You will reveal only the password for the outer volume, not for the hidden one. Files that really are sensitive will be stored on the hidden volume.

2) No TrueCrypt volume can be identified (volumes cannot be distinguished from random data). As of TrueCrypt 4.0, it is possible to write data to an outer volume without risking that a hidden volume within it will get damaged (overwritten). When mounting an outer volume, the user can enter two passwords: One for the outer volume, and the other for a hidden volume within it, which he wants to protect. In this mode, TrueCrypt does not actually mount the hidden volume. It only decrypts its header and retrieves information about the size of the hidden volume (from the decrypted header). Then, the outer volume is mounted and any attempt to save data to the area of the hidden volume will be rejected (until the outer volume is dismounted).

# Encryption

## Chapter 4

# Encryption

**How Encryption Works** - Encryption is based on prime numbers - two prime numbers to be exact. When multiplied together, two prime numbers will yield a product that is only divisible by one and itself – and those two prime numbers. These prime numbers are used in a complex algorithm to scramble (encrypt) a message or file. Thereafter, the two prime numbers are needed again in order to unscramble (decrypt) the message or file. An example is shown below:

| | | |
|---|---|---|
| | 12,313 | Prime Number 1 |
| X | 45,613 | Prime Number 2 |
| | 561,632,869 | Product |

**Bit's Explained** – All data stored on a computer (including prime numbers) is converted to hexadecimal and then to binary format. A binary format is a "0" or a "1". The "0" or "1" is represented as a "positive" or "negative" charge on a computer's hard drive, or as a small of large pit (hole) on a CD ROM. From example the letter "A" is represented on your computer's hard drive as "0100 0001". Here is the complete alphabet and numbers 1 through 15 represented in binary code.

**The Alphabet in Binary Code**

| Letter | Binary Code | Letter | Binary Code |
|---|---|---|---|
| A | 01000001 | a | 01100001 |
| B | 01000010 | b | 01100010 |
| C | 01000011 | c | 01100011 |
| D | 01000100 | d | 01100100 |
| E | 01000101 | e | 01100101 |
| F | 01000110 | f | 01100110 |
| G | 01000111 | g | 01100111 |
| H | 01001000 | h | 01101000 |
| I | 01001001 | i | 01101001 |
| J | 01001010 | j | 01101010 |
| K | 01001011 | k | 01101011 |
| L | 01001100 | l | 01101100 |
| M | 01001101 | m | 01101101 |
| N | 01001110 | n | 01101110 |
| O | 01001111 | o | 01101111 |
| P | 01010000 | p | 01110000 |
| Q | 01010001 | q | 01110001 |
| R | 01010010 | r | 01110010 |
| S | 01010011 | s | 01110011 |
| T | 01010100 | t | 01110100 |
| U | 01010101 | u | 01110101 |
| V | 01010110 | v | 01110110 |
| W | 01010111 | w | 01110111 |
| X | 01011000 | x | 01111000 |
| Y | 01011001 | y | 01111001 |
| Z | 01011010 | z | 01111010 |

Here are the numbers from 0 to 15, in binary:

0000 = 0
0001 = 1
0010 = 2
0011 = 3
0100 = 4
0101 = 5
0110 = 6
0111 = 7
1000 = 8
1001 = 9
1010 = 10
1011 = 11
1100 = 12
1101 = 13
1110 = 14
1111 = 15

As you can see in the chart above, 8 bits of data are required to record a single letter, or number greater than 15. Therefore if you have a 40-bit encrypted password, you really have a 5 character password. 56 bit, 64 bit, and 128 bit encrypted passwords translate to 7, 8 and 16 character passwords. In other words, when you use 128 bit encryption, this means that you are using prime numbers that are 16 digits in length to generate the basis for scrambling your data.

**The Size of the Prime Numbers** - The size of the prime numbers used dictate how secure the encryption will be. A message encrypted with 5 digit prime numbers (40-bit encryption) yields about 1.1 trillion possible results. A message encrypted with 7 digit prime numbers (56-bit encryption) yields about 72 quadrillion possible results. However using 128-bit encryption (16 digit numbers) yields 340,282,366,920,938,463,463,374,607,431,768,211,456 possible results. Mathematically, It would take a super computer testing 100 billion passwords per second, 107,829 billions years to break 128-bit encryption using brute force. (Today's fastest chips can handle about 256 million encryptions per second.)

**Time Needed To Crack** - Mathematically speaking, based upon today's top computing power 40-bit, 56-bit, 64-bit, and 128-bit encryption could be broken in 1 second, 19 hours, 7 months and 11,000 quadrillion years, respectively. This is why 128-bit encryption is the standard used world-wide to protect financial transactions and sensitive data.

| Key Length (bits) | 1995 | 2000 | 2005 |
|---|---|---|---|
| 40 | 68 seconds | 8.6 seconds | 1.07 seconds |
| 56 | 7.4 weeks | 6.5 days | 19 hours |
| 64 | 36.7 years | 4.6 years | 6.9 months |
| 128 | 6.7e17 millennia | 8.4e16 millennia | 1.1e16 millennia |

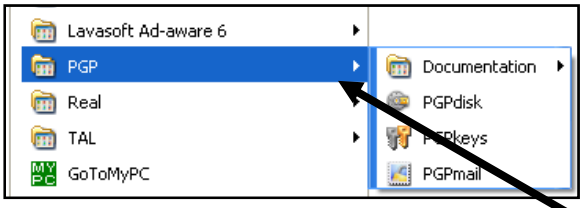
Table of time needed to break certain key sizes using hardware
http://www.cs.bris.ac.uk/~bradley/publish/SSLP/chapter3.html

It has been estimated that 128-bit encryption will be breakable in about 105 to 125 years (by the years 2109 to 2129).

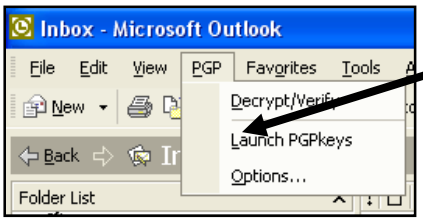
**Letters versus Numbers** - You might be interested to know that four words selected at random are much more effective than 56 Bit encryption. According to Jeremy Bradley of the University of Bristol, a 7-character password (56-bit) has 1,028,071,702,528 possible results. However four random words yield a total of 390,625,000,000,000,000 possible results. His basis for this claim is explained here: http://www.cs.bris.ac.uk/~bradley/publish/SSLP/chapter3.html.

## PGP (Pretty Good Privacy)

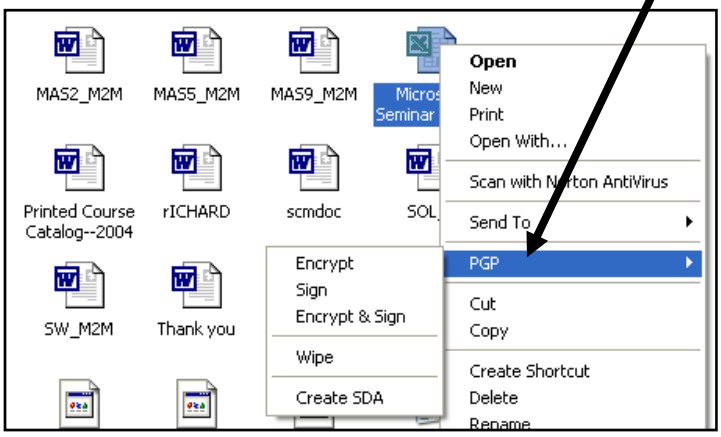

PGP or Pretty Good Privacy was released on June 5, 1991. Developed by Phil Zimmerman, Phil first sent PGP to Allan Hoeltje and then Kelly Goen who in turn released PGP through Internet user groups. This set off an unexpected feeding frenzy. Volunteers around the world offered to help Phil port PGP to other platforms, add enhancements, and generally promote the product. Fifteen months later, in September 1992, PGP 2.0 was released for MSDOS, Unix, Commodore Amiga, Atari, and a few other platforms, and in about ten foreign languages. Shortly thereafter US Customs took an interest in the case. At first the government tried to build a case against Phil for exporting weapons outside the US, and they frequently harassed him. By doing so the government helped propel PGP's popularity by igniting controversy that would eventually lead to the demise of the US export restrictions on strong cryptography. Today, PGP remains just about the only way anyone encrypts their email. And now there are a dozen companies developing products that use the OpenPGP standard. You can download PGP for free, or purchase a more feature rich version at this web site: www.pgp.com. Here is a quick introduction into using PGP:








Once installed, PGP shows up as an application in your Start Button, an Icon in your System Tray, an icon in Outlook, and as a right mouse click in Explorer.



To start using PGP, launch the product and start the wizard to generate the encryption keys as shown below:


The PGP wizard shown above walks you through the process of creating your encryption keys. Once you have created an encryption key, you can encrypt text, files, folder, or e-mails using that newly created PGP encryption key. Presented below is an example of a simple message before and after encrypting with PGP.

**Original Message**

```
My credit card number is 487654876458764
```

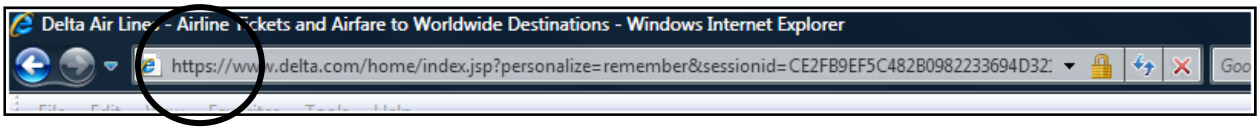
**Same Message as Above - Encrypted with a PGP 128 Bit Key**

```
-----BEGIN PGP MESSAGE-----
Version: PGP 8.0.3 - not licensed for commercial use: www.pgp.com
qANQR1DBwU4DWpD/xXWUSrgQB/9YzTEgIeaWWWGwI7QbZSADfxjiNYcIv9MgXkGN
EeiSjbbanr4LeVylp5CIwByQSipY1FWVuCfZimxwNsmlG8y3JpS8Hpu94/FpCruv
6w4fepg/eSbJaF6hxGegjjWXur3lMK0tPZVnp8eOTrgaz+787y1YPr5yVYUYDx1V
FN1Dh2XDUiKMU9BcfxAwbgm6EnkZqbo04tDQqUTMG5TLwYcL6Z7D+AUhDOiZWHl5
yjgj4heSuwkeCybAHA1ivAApAf8h1QTHZG5YUbF5jn9xZvM9q5Nv1a3vpDyzICQI
246b5hBTlpzJiFsbI9QJ59MeiQnYxWrc7A5NwrMUMV/mQmejB/9ZJS4KiK4Jb7+J
rkjYHqVvWrMYapDQN2nRhtFKxj9GTHqE5J9HgFRX5NoUooMOk8PTaOynivQtUMUF
9XkUdrJv+jz+rTuJA8UieDLPsfme0P9qcV/2seP1i6lhDJ7j7RcbnJZKw4ebR25y
S167lNARclnixXB9q7LDieAnJWZ//fGOoa8PXf9AaOUmD1x9qSvOAriBAduw6L1D
CqHpuRNsQM55YeIol6jjucqEZV0p4mrDkf1F9SxiVAKThly5aOdA/U4klr3rBFRH
FhogPngpRotbXt0XArxbf6sIj0a6VgpThSlyTcFNjFekD3bKAcCC0XrPhZzTO8cP
7kxpBL8t0lkBD5kRRBVpO618s31GIv1CSuwkTL2mdkej5meinYXZVmspp6TNu/V9
fsqto+AWZzxIwQtGOEJ1CEI/H4hwt/TYTTHOvwyNDx7McZfMYQmnVoh0jcYQV7V4
og===gWVJ
-----END PGP MESSAGE-----
```

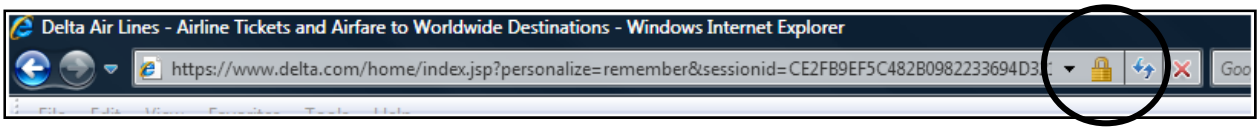
It is important to point out that an encrypted message is still naked and wide-open on the internet or on a computer hard drive – it's just that now no one can make sense of that message/file/e-mail without the proper decryption key.

**PGP's Two Key System** - PGP is based on public key cryptography, a widely accepted and highly trusted public key encryption system, by which you and other PGP users generate a key pair consisting of a **'private key'** and a **'public key'**. As its name implies, only you have access to your private key, but in order to exchange files with other PGP users you need a copy of their public key and they need a copy of yours. You use your private key to sign the file attachments you send to others and to decrypt the files they send to you. Conversely, you use the public keys of others to send them encrypted files and to verify their digital signatures. PGP won't route your e-mail over a Secure Socket Layer (SSL), but it will be unreadable by anyone other than you and the person to whom it is addressed. Keep in mind that encryption is for the message body only - it does not hide the subject line or the headers.

**SSL – A Web Based Version of PGP's Two Key System -** One popular implementation of public-key encryption is the Secure Sockets Layer (SSL). Originally developed by Netscape, SSL is an Internet security protocol used by Internet browsers and Web servers to transmit sensitive information. SSL recently became part of an overall security protocol known as Transport Layer Security (TLS).




Look for the "s" after "http" in the address whenever you are about to enter sensitive information, such as a credit-card number, into a form on a Web site. In your browser, you can tell when you are using a secure protocol, such as TLS, in a couple of different ways. You will notice that the "http" in the address line is replaced with "https," and you should see a small padlock in the status bar in the browser window.



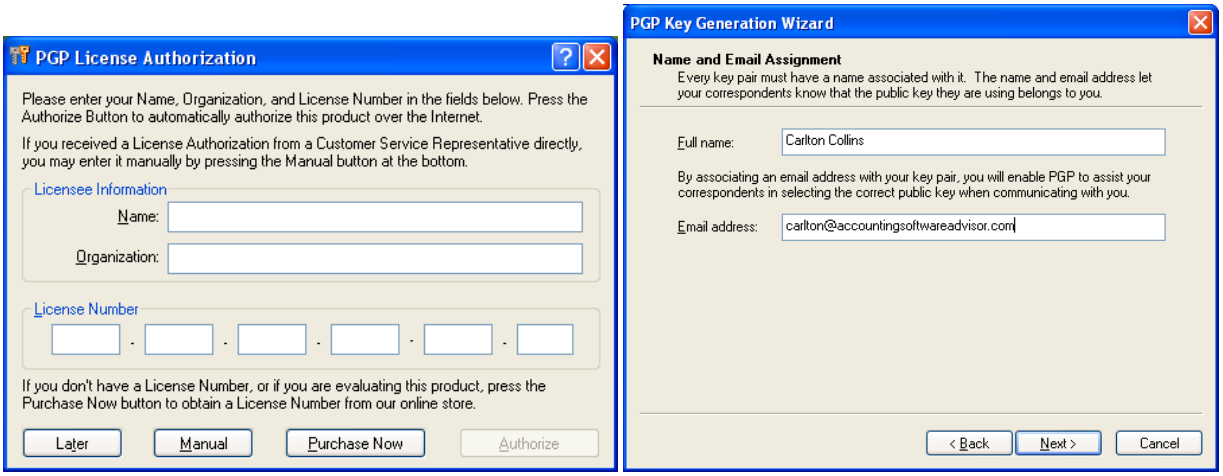

The padlock symbol lets you know that you are using encryption. Basically what this means is that a private key has been generated by the server you are accessing, and has been sent to your computer and is being held in RAM until needed. Once you have entered the information you want to send and press the SUBMIT button, the key is used to encrypt the message and the data is sent to the web server, or in the case shown above – the Delta Airlines web server.

Public-key encryption takes a lot of computing, so most systems use a combination of public-key and symmetry. When two computers initiate a secure session, one computer creates a symmetric key and sends it to the other computer using public-key encryption. The two

computers can then communicate using symmetric-key encryption. Once the session is finished, each computer discards the symmetric key used for that session. Any additional sessions require that a new symmetric key be created, and the process is repeated.

**Is Big Brother Watching You Anyway? -** When PGP was first developed, it was understood that the only person capable of reading an e-mail encrypted with PGP was the e-mail recipient. While unconfirmed, it is suspected that since PGP was purchased from Phil Zimmermann, its developer, by Network Associates, Inc. (NAI) several years ago, that a 'master key' exists in the hands of both NAI and the U.S. Federal Government. Even with this in mind, PGP is just about the safest and most reliable method of encryption available.

In October, 2001, NAI put PGP up for sale. With no buyers, in March of 2002 NAI dropped support and development of its PGP desktop encryption software. On August 19, 2002, NAI sold PGP to PGP Corporation, a newly formed company. The deal gives the new company a line of encryption products based on the PGP algorithm, including PGPmail, PGPfile, PGPwireless, PGPkeyserver, for the Windows and Macintosh operating systems. A full history of PGP can be found at [www.pgp.com/company/pgphistory.html](www.pgp.com/company/pgphistory.html)

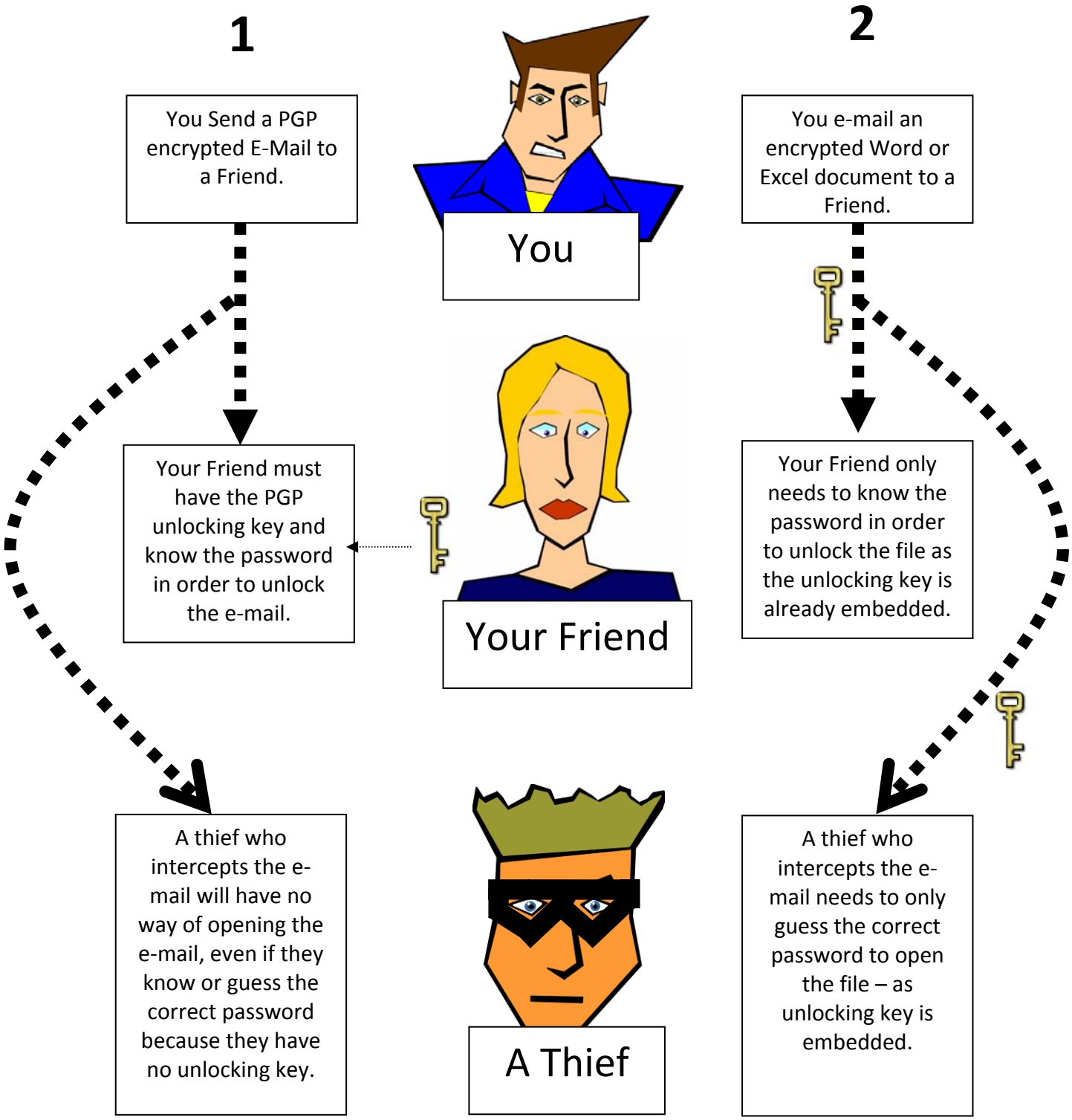



Though a freeware version of PGP does exist, the End User License Agreement (EULA) is rather restrictive limiting it to home-based non-profit use. Freeware PGP set-up only takes a few minutes, but users should note these facts about the free version of PGP:

- Does not include automatic encryption of email file attachments
- Does not provide plug-in integration with Outlook, Outlook Express, and other email applications
- Does not operate with PGP Admin or other PGP deployment tools

## Self Decrypting Files

Some implementations of encryption are self-decrypting – which means that the unlocking key needed is already embedded in the file – all you need is the password to activate the unlocking key. Consider the following two examples:



## E-Mail Encryption Software

**PKWARE's SecureZip** (www.pkware.com) ($30) – It does automatically encrypt e-mail, as well as Office files. Save and send files securely directly from Microsoft Office® applications, including Word®, Excel®, and PowerPoint® Secure and compress emails and attachments in Microsoft Outlook®. Encrypt data using passphrases, X.509 digital certificates, or both.

**Google Message Encryption, (formerly Postini)** (www.google.com) - Hosted solution that automatically encrypts email based on your policy definitions, helping your organization avoid the financial penalties and brand equity damage that can result from sending proprietary or regulated data via unprotected email. Send encrypted messages to business partners and customers. No additional software, hardware or technical training required. Automated or user-initiated encryption for confidential emails to any recipient. Centralized reporting of encrypted messages and policy enforcement. Centrally-managed content inspection, encryption policies to help comply with GLBA, HIPAA, PCI DSS and Data privacy regulations.

**Entrust** Email Encryption (www.entrust.com) - Protects private, sensitive and valuable information communicated via email. Email encryption can be deployed using email encrypting software, secure email servers or secure webmail centers. Entrust email encryption solutions work with a broad range of email applications including Microsoft® Outlook/Exchange and Lotus® Notes/Domino. It can be used by mobile users including those with RIM BlackBerry® handheld devices and via secure web mail. Entrust email encryption software uses S/MIME, PGP and Entrust encryption formats. Benefits: Transparent, easy-to-use email security; Automatic encryption and digital signatures; Integration with content analysis tools for email compliance; 'Government strength' security validated against NIST standards.

**ShyFile** ($59) - Make up a 32 character key entry, Enter the text you wish to encode, Attach secure ShyFile to your email, Recipient simply uses a browser to decode. The unlocking key is embedded in the file. ShyFile encodes your text (txt- and html-files) and packs it into an extra file that is to be attached to an outgoing email or uploaded to a website. The recipient thereof

does not need to have ShyFile installed to be able to decode since any Internet browser will open it and prompt the user to enter the matching key phrase before decoding it. ShyFile also encrypts binary files, which require a free demo version of ShyFile to decode though. Simple 1on1 symmetric key entries are used, no Public and Private Keys. ShyFile exclusively uses its own independently developed TL6144D algorithm, offering a depth of encryption of up to 6144bit. That reaches or even tops military requirements. A File Shredder is included to thoroughly delete a file on your hard drive in a way no un-delete tool could ever restore it again. ShyFile works independently from all your web based email accounts and desktop email applications.

**AnchorMail** (www.anchormail.com) Secure email solution provides a service-based approach for encrypting ad hoc emails and securely delivering the messages to any inbox, AnchorMail enables any enterprise to enforce message policies and/or client-initiated trusted e-communications that can be securely delivered to any recipient, without requiring the receiving party to download or install any software. The AnchorMail service is responsible for the data management, key management, user enrollment, online opening, and secure reply, in addition to related administrative functions (operations, backup, availability, etc.). This removes the deployment integration and lifecycle management of a typical secure email offering, and thus decreases the costs of resources, time, and administration.

**Secure Hive** (www.securehive.com) ($86) - Secure Hive is a tool for secure archiving and sharing of files. It enables you to create encrypted archives and self-extracting .exe files for secure storage and file sharing. It also includes a means of encrypting parts of, or entire, documents, email messages, etc. Secure Hive offers the enterprise a method of: Securing sensitive documents; protecting information during transfer; Securing emails.

**CenturionMail** (www.centurionsoft.com) ($59) - Windows based utility to send encrypted information by email. Recipients of encrypted messages receive an attachment to the email which when executed requires the user to enter a password to open it. CenturionMail is integrated in MS Outlook. One button operation within the Outlook composing window is all that is needed to send an encrypted email. Users of other email programs can still use the program through the CenturionMail interface which calls to the default email program. Supports all version of MS Outlook including Outlook 2003. Encrypted files can be sent as ZIP, CAB, or our new custom defined extension. AES: Now offering stronger 256 bit, open source encryption. Password Manager: Securely store and manage all the passwords to be used for various recipients. When using the Microsoft Outlook plug-in, it will pre-fill the default password for any recipient in the Password Manager. Password hints can also be saved and automatically sent. Shredder: Securely delete files and folders either during the encryption process (deletes the non-encrypted originals) or separately. On-the-Fly Encryption: Automatically encrypt a local copy of the files or folders being sent.

**GnuPG** www.gnupg.org (Free) - Free Software Foundation, Inc. offers GnuPG, (GNU Privacy Guard) a complete and free replacement for PGP. Because it does not use the patented IDEA algorithm, it can be used without any restrictions. GnuPG is a RFC2440 (OpenPGP) compliant application. GnuPG itself is a command line tool without any graphical stuff. It is the real crypto engine which can be used directly from a command prompt, from shell scripts or by other programs. Therefore it can be considered as a backend for other applications.

## Conclusions

1. You should assume that every e-mail you send has been read by more than 1,000 people. This is because all unencrypted e-mails are naked and wide open to the world. A simpler Sniffer tool can capture your packets and reassemble your e-mails.

2. PGP was the first computer based encryption tool, although the existence of coded messages (or cryptography) has been verified as far back as the Roman Empire.

3. Encryption works on primed numbers. According to Bill Gates in his book "The Road Ahead", there are more prime numbers of adequate size and length than there are Atoms in the universe.

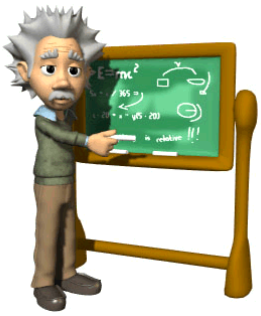
4. Data on your computer is stored in binary code called "bits, which means zero's and one's. These Since it takes 8 bits to represent a number or letter, it takes 40 bits to represent 5 numbers or letters, or 128 bits to represent 16 numbers or letters. Hence when you work with 128 bit encryption this means that you are actually working with 16 digit prime numbers.

5. Using today's technology, it would take about 11,000 quadrillion years to break a 128 bit encrypted message.

6. To protect your e-mails with encryption, you and your e-mail pal could install PGP.

7. Upon installing PGP, you would need to generate a set of encryption keys, and send your locking key (private key) to your pal. You pal would do likewise sending their locking key to you. Thereafter, all e-mails sent to one another (including attachments) would be absolutely encrypted with 128 bit encryption.

8. It is widely rumored that the US government secretly holds a universal code for unlocking all PGP keys. At least this makes for a good conspiracy theory.



# Strong Passwords & Password Management

## Chapter 5

**One Password or Multiple Passwords?**

Do you have one catch-all password that you use everywhere or do you create a new password for every different account, website, file, and relationship you deal with? It is a perplexing question but almost everyone agrees that the use of a single password everywhere is foolish. An RSA survey shows that 58% of users have more than six passwords, and half of those have thirteen. Here's why:

1. If one company can see the password you use for their account, an unscrupulous employee might attempt to use that same password and e-mail address to access your Amazon account, Pay Pal account, or Credit card account.

2. From time to time it is necessary to provide a friend or associate with your password information – for example to edit your web site. If you use the same password for your web site and bank account, then your friend or colleague may be armed with information that could be used to compromise your identity.

3. Passwords tend to last for years with some accounts –if your password does manage to get out in the open, it might be a nightmare to change all known passwords for all of your accounts, e-mails addresses, web sites, etc.

Although managing multiple passwords has it's own set of problems, it is widely considered to be a better strategy than using one or a few passwords across multiple accounts.

**Creating Strong Passwords**

In most cases, when people who find out too late that their passwords have been compromised, it is usually because they were simply too easy to guess. It's not so hard to create a strong password... here are some tips to make the keys to your identity a tougher lock to pick.

1. **At least 12 Characters -** As the length of your password increases it's harder to crack it. Most people recommend a minimum of 8 characters, but anything more than that makes it even more secure. I like to use at least 12 characters.

2. **Letters & Numbers -** Combining letters, numbers and special characters makes your password much harder to guess. Using a password that's easy for you to remember may also be an easy password for an identity thief to guess. But there's a delicate balance... you want passwords that simple for you to remember, but difficult for others to guess.

3. **Use all Lower Case –** It is true that you can add complexity by alternating between upper and lowercase letters. However, these will be harder to remember, read, and type correctly. Further, uppercase letters require two hands to be used for the shift key. I find that this is too frustrating to mix case and therefore and I always try to use lowercase letters for all of my passwords.

4. Some people like to substituting special characters for letters and numbers such as the "$" instead of an "S" or a "1" instead of "I". Once again, I find this too frustrating to remember, read, and type. I don't recommend this.

5. To make password both hard to crack and simple to remember, I have some standard words that I embed in front and behind my passwords. For example, my Delta Airlines, AVIS, and Marriott passwords might look something like this:

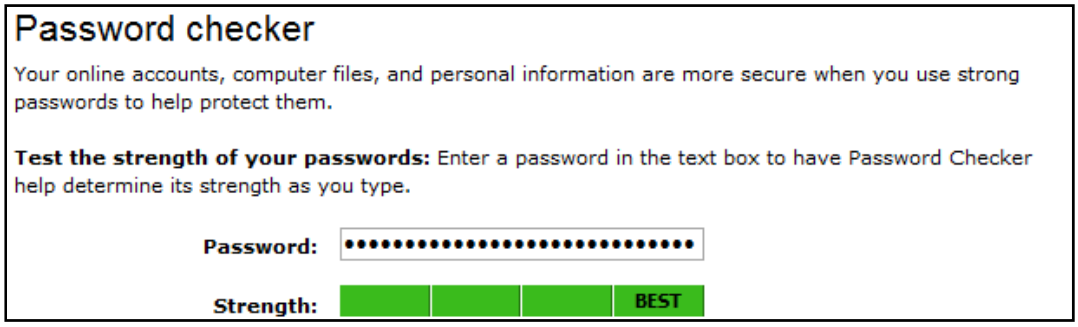
    a. delta5544summer6388947+
    b. avis3319summer6388947+
    c. marriott2298summer6388947+

    Each password has 5 parts :

    1. the beginning part "delta" for Delta Airlines;
    2. the second part "5544" is four randomly chosen numbers;
    3. the word "summer" is a common word I always throw in,
    4. the number "6388947" is my childhood telephone number;
    5. and for good measure I throw a "+" sign on the end.

    Using this approach, all I really have to remember is the 4 random numbers (like a PIN) in part 2, the other 4 parts I can easily remember. This way I can usually recreate my password from memory, but a hacker or hacking program would take billions of years to break the password in its totality.

The Microsoft Password Checker which is available online tells me that the strength of these passwords are excellent – see for yourself:




http://www.microsoft.com/protect/yourself/password/checker.mspx

### Bad Passwords

Password pitfalls include using your name, child or pet's name, your birthday or other information that may be linked with your identity. Also steer clear of no-brainers like "abc123" or "password" as your password. Hackers recently created a fake Myspace login page, and collected over 34,000 passwords before the ruse was detected. Because the data was left on a public server for some time, it proved to be an interesting real-world case study on BAD passwords. Analysis of this data showed some surprising results -- almost one percent of Myspace users had the word "password" in their password. With over 100 million Myspace users, that's a MILLION easily-guessed passwords!

Other popular "words" used in passwords included: abc, baseball, football, iloveyou, myspace, monkey, princess, qwerty, soccer, superman, and 123456. It was also common to add a number to the end of these words, such as abc123 or baseball1. Profanities also occurred with a high frequency in passwords. Your takeaway: don't use these words, or variants of them in your password, or you'll be making it that much easier for Evildoers to guess their way into your private information.

### Changing Passwords Regularly

Changing passwords on a regular basis will help to ensure that you are maintaining a high level of security. Personally I believe that this measure is not cost effective as it takes far too much time to change, record, and edit the proper documentation so that you can find the right password later. However, in some workplace settings, login passwords must be changed every 30 days. Whatever interval you choose, be careful not to use a predictable pattern for your passwords, such as AxxxxxA / BxxxxxB / CxxxxxC or JANxxxx / FEBxxxx / MARxxxx. This is important because an intruder may not leave tracks. If someone has guessed your password, you can at least make sure they won't have long term access to your data.

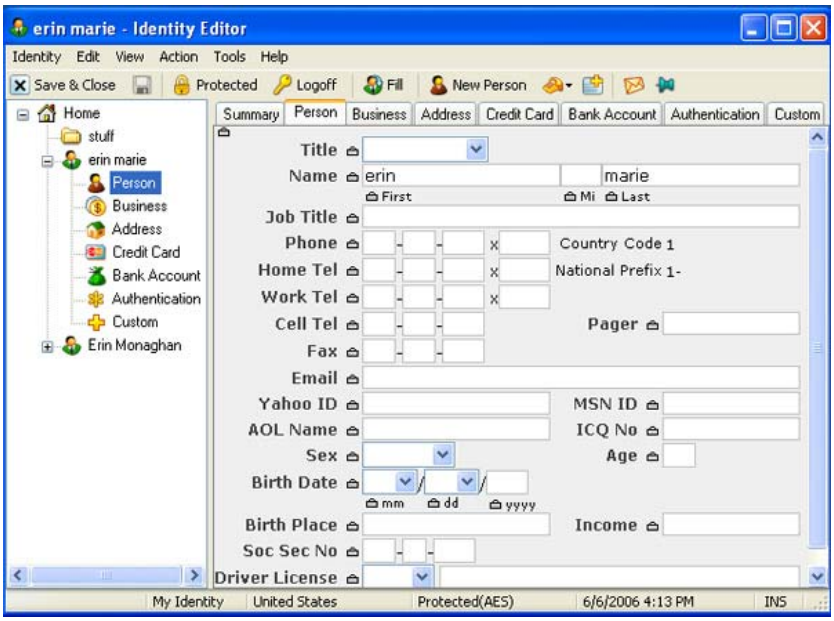
### Managing Passwords

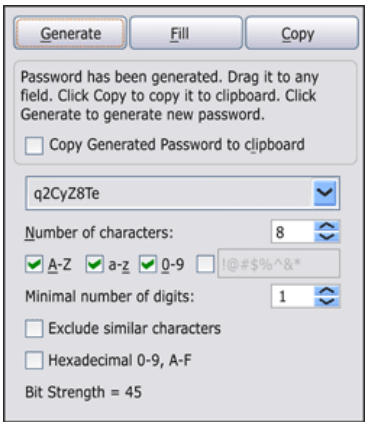
Storing an unprotected list of passwords on your computer is not a good idea, however if you store them in a very well protected Excel or Word document (password protected with a very strong password), then you are fine in my opinion. However, you also have the option of using a Password Manager Tool to help you keep track of these passwords. A password manager is software that helps a user organize passwords and PIN codes. The software typically has a local database or files that hold the encrypted password data. Many password managers also work like a form filler, thus they fill the user and password data automatically into forms. Some have password generator capabilities. In view of the rising threat of Phishing, password managers are also used as the best defense against such threats. Unlike human beings, a password manager program, which can handle automated login script, is not susceptible to visual imitations and look-a-like websites. With this built in advantage, the use of a password manager is beneficial to everyone, even if he or she only has a few passwords to remember. However, one must keep

in mind that not all password managers can automatically handle the more complex login procedures now imposed by banking websites.

For example Roboform (Free to $35) is a top-rated Password Manager and Web Form Filler that automates password entering and form filling. RoboForm was named PC Magazine Editor's Choice, and CNET Download.com's Software of the Year. RoboForm does the following:

1. Memorizes your passwords and Logs You In automatically.
2. Fills long registration and checkout forms with one click.
3. Encrypts your passwords to achieve complete security.
4. Generates random passwords that hackers cannot guess.
5. Fights Phishing by filling passwords only on matching web sites.
6. Defeats Keyloggers by not using keyboard to type passwords.
7. Backs up your passwords, Copies them between computers.
8. Synchronizes passwords between computers using GoodSync.
9. Searches for keywords in your passwords, notes and Internet.
10. Portable: RoboForm2Go runs from USB key, no install needed.
11. PDA-friendly: sync your passwords to Pocket PC and Palm.
12. Neutral: works with Internet Explorer, AOL/MSN, Firefox.
13. IE 7 and Vista are now supported.




**Password Manager XP** is a program to store passwords. It claims to rid computer users of the headaches caused by lost passwords, forgotten access codes and other sensitive information. With this program, you safely store all your logins, passwords, PIN codes, credit card numbers, access codes, files, and any other confidential information in one place. The product allows you to create several databases for storing desired information. Each database has its own access password and is encrypted with the algorithms of your choice. This means capability to apply several different encryption algorithms at a time, which significantly increases protection against unauthorized access of your data. Besides, the program comes with an option to automatically exit databases when idle for a set period of time, which decreases the likelihood of stealing your data when leave your computer with application running (for example, you have been distracted by other things or simply forgot to quit the program).

KeePass is a free/open-source password manager or safe which helps you to manage your passwords in a secure way. You can put all your passwords in one database, which is locked with one master key or a key-disk. So you only have to remember one single master password or insert the key-disk to unlock the whole database. The databases are encrypted using the best and most secure encryption algorithms currently known (AES and Twofish). It allows you to organize your entries into categories and offers several ways to conveniently enter your username/password; you can use drag and drop, copy to the clipboard, or create auto-type sequences that can enter the login information with a single click.

The Firefox browser also has a rudimentary password keeper and has a master password option. Internet Explorer will remember passwords, but lacks the master password option. Social engineering, phishing, and even careless oversight by internet service providers are yet other ways that a hackers might get your password. Read more about Phishing Scams to avoid voluntarily providing your password via deceit and falling victim to Identity Theft.

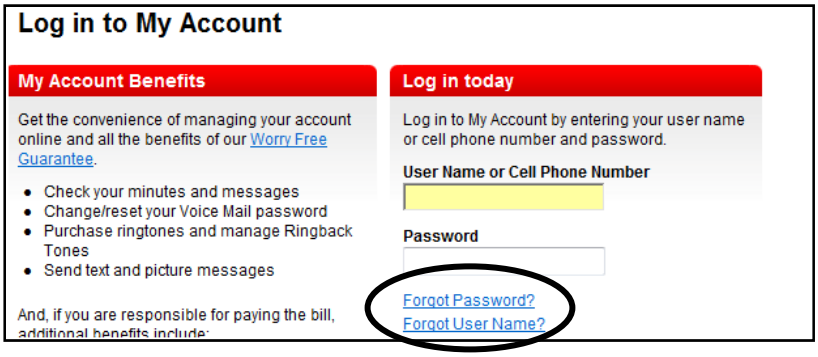
## Password Fatigue

Password fatigue describes the syndrome where people are required to remember an excessive number of passwords as part of their daily living. The increasing prominence of information technology and the Internet in employment, finance, recreation and other aspects of people's lives, and the ensuing introduction of secure transaction technology, has led to people accumulating a proliferation of accounts and passwords. According to British online-security consultant NTA Monitor the typical intensive computer user has 21 accounts that require a password.

Aside from contributing to stress password fatigue may encourage people to adopt habits that reduce the security of their protected information. For example, an account holder might use the same password for several different accounts, deliberately choose easy to remember passwords that are vulnerable to cracking, or rely on written records of their passwords.

## Password Recovery

The majority of password protected web sites provide password recovery that allows users to recover their passwords via email. Sometimes this is automated via the web site, although some web sites (especially paid-for or 'high value' web sites) may require additional checks via customer service operators. According to a PBS report, a survey of customer service representatives revealed that about 20% of the CS calls from users are about problems with passwords.




Be aware that if someone has access to your computer for a few moments, they could access your online account, click the lost password button, and have the password resent to your computer's e-mail. There they could quickly learn your password, and then delete the e-mail to erase their tracks.

# Windows Security

## File & Folder Security

## Chapter 6

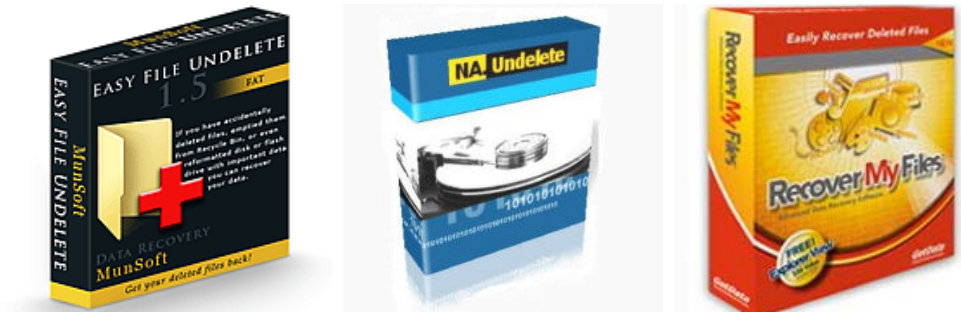
## FAT32 versus NTFS

1. **You Must Choose** - When you format your hard drive, you must choose to use either FAT32 (**F**ile **A**llocation **T**able 32) or NTFS (the Windows **NT F**ile **S**ystem).


2. **Do Not Choose FAT 32 –** because FAT32 does not offer any security.

3. **Do Choose NTFS** – NTFS allows you to password protect files, password protect folders, and to apply encryption to your hard drive using EFS (**E**ncryption **F**ile **S**ystem).

4. **Deleted Files** - When using FAT32, deleted files are not really deleted. They are only renamed in the File Allocation Table (from "Budget.xls" to "*udget.xls". The asterisk prevents the file name from being viewed, but the file still exists on the hard drive. Many available tools enable you to rename the file replacing the asterisk with a letter or number, and then the file is completely visible again.




With NTFS, when you delete a file, the file's location on the hard drive is overwritten, and there is not recovery option.

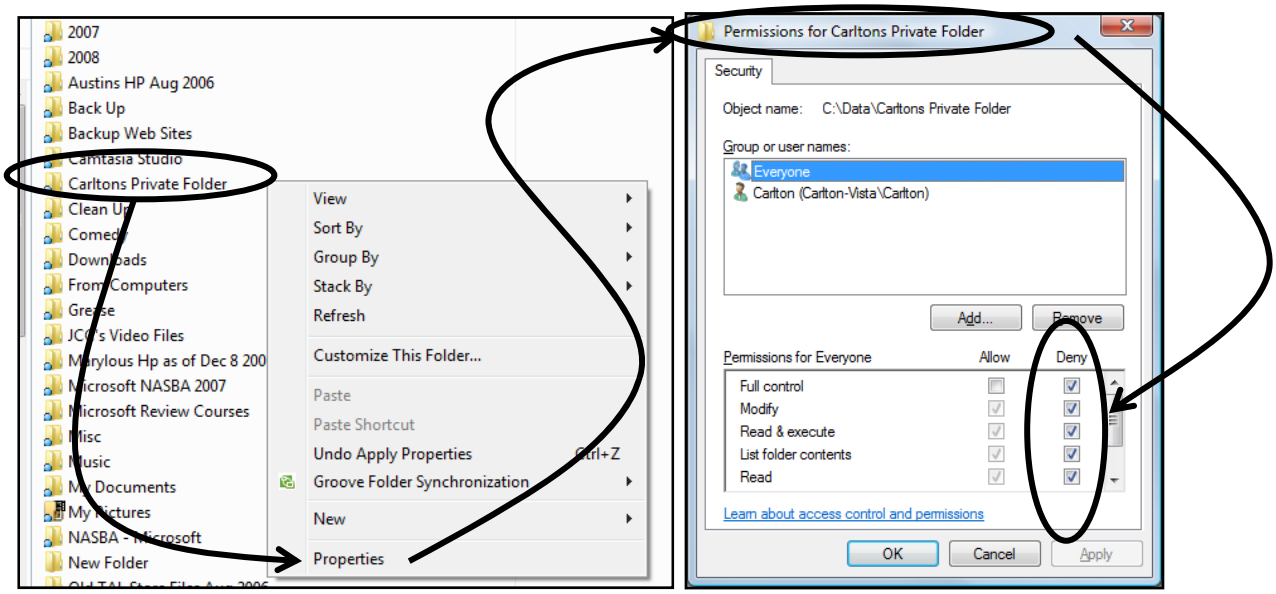
5. **No Impact on Network** – Choosing FAT32 or NTFS has no impact on sharing data across a network.

6. **NTFS is Also Better in Other Ways** – NTFS supports larger files, larger drive partitions, has better data compression, and has less file fragmentation.

7. **It's Easy to Change to NTFS -** If you are not already using NTFS, you can change to NTFS rather easily. You can switch to NTFS without reformatting your hard disk and restoring your apps and data from a backup. Just choose Start, Run, type cmd.exe, and press <Enter> to open a Command Prompt window. Now type **<convert c: /fs:ntfs>** (without the brackets) to convert your C: drive to NTFS.

## File & Folder Security

To configure the security and permissions of a file or folder, right-click the file or folder and select the "Sharing and Security" or "Properties" option.




In the example above the folder named "Carlton's Private Folder" has been protected by denying access to everyone (except the user "Carlton"). Now, no one on the network or on the computer will see the folder or have access to the folder and its contents unless they are logged in as the user "Carlton".

**Warning - Hidden Files and Folders Can Still Be Deleted -** Please be aware that even though the folder is hidden from view, groups or users who are granted Full Control on a parent folder can delete any files in that folder regardless of the permissions protecting the file's access.

**Warning - Anonymous Users Do Not Belong to Everyone** - In Windows Vista and Windows Server 2003, by default the Everyone group does not include the Anonymous group, so permissions applied to the Everyone group do not affect the Anonymous group. You must apply those permissions separately.

## File and Folder Permissions

The following table lists the access limitations for each set of special NTFS permissions.

| Special Permissions | Full Control | Modify | Read & Execute | List Folder Contents (folders only) | Read | Write |
|---|---|---|---|---|---|---|
| Traverse Folder/Execute File | x | x | x | x | | |
| List Folder/Read Data | x | x | x | x | x | |
| Read Attributes | x | x | x | x | x | |
| Read Extended Attributes | x | x | x | x | x | |
| Create Files/Write Data | x | x | | | | x |
| Create Folders/Append Data | x | x | | | | x |
| Write Attributes | x | x | | | | x |
| Write Extended Attributes | x | x | | | | x |
| Delete Subfolders and Files | x | | | | | |
| Delete | x | x | | | | |
| Read Permissions | x | x | x | x | x | x |
| Change Permissions | x | | | | | |
| Take Ownership | x | | | | | |
| Synchronize | x | x | x | x | x | x |

# File Sharing Permissions

1. **Share Permissions versus NTFS Permissions** - Share permissions and NTFS permissions are independent in the sense that neither changes the other. The final access permissions on a shared folder are determined by taking into consideration both the Share permission and the NTFS permission entries. The more restrictive permissions are then applied.

2. **Windows XP Home and Windows Vista Home Users –** Are limited to Share permissions only.

3. **Using Share with FAT32** - Share permissions are often used for managing computers with FAT32 file systems, or other computers that do not use the NTFS file system.

4. **Standard Operating Procedure -** Many experienced administrators prefer to set share permissions to “Full Control for Everyone”, and to rely entirely on NTFS permissions to

restrict access. This frees you from having to think about Share permissions, but NTFS permissions are more complex than Share permissions.

5. **Four Folder Types** – Four different types of folders can be setup using "Share" or "NTFS" Permissions, with slight differences as the table below shows:

| Folder type | Share permissions | NTFS permissions |
|---|---|---|
| **Public folder**. A folder that can be accessed by everyone. | Grant Change permission to the Users group. | Grant Modify permission to the Users group. |
| **Drop folder**. A folder where users can drop confidential reports or homework assignments that only the group manager or instructor can read. | Grant the Change permission to the Users group.<br>Grant the Full Control permission to the group manager. | Grant the Write permission for the users' group that is applied to **This Folder only**. (This is an option available on the **Advanced** page.)<br>If each user needs to have certain permissions to the files that he or she dropped, you can create a permission entry for the Creator Owner well-known security identifier (SID) and apply it to **Subfolder and files only**. For example, you can grant the Read and Write permission to the Creator Owner SID on the drop folder and apply it to all subfolders and files. This grants the user who dropped or created the file (the Creator Owner) the ability to read and write to the file. The Creator Owner can then access the file through the **Run** command using *\\ServerName\DropFolder\FileName*.<br>Grant the Full Control permission for the group manager. |
| **Application folder**. A folder containing applications that can be run over the network. | Grant Read permission for the Users group. | Grant Read, Read and Execute, and List Folder Content permissions to the Users group. |
| **Home folders**. Individual folders for each user. Only the user has access to the folder. | Grant the Full Control permission to each user on their respective folder. | Grant the Full Control permission to each user for their respective folder. |

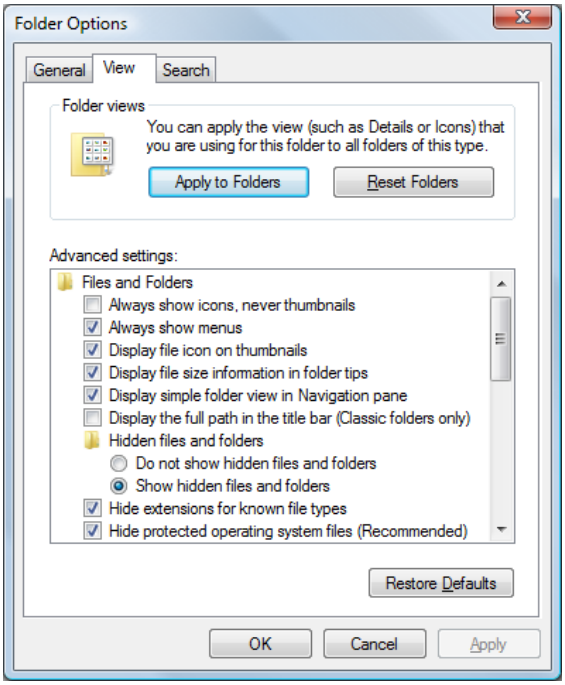
   a. NTFS permissions affect access both local and remote users.

   b. Share permissions apply only to network shares.

   c. Share permissions do not restrict access to any local user, or to any terminal server user, of the computer on which you have set Share permissions. Thus, Share permissions do not provide privacy between users on a computer used by several users, nor on a terminal server accessed by several users.

## Folder Settings

You can apply many settings to each folder by selecting the Tools, Options from the Folder menu. Four of these settings have a security impact as follows:




1. **Hide Hidden Files -** One option allows you to display or hide hidden files or hidden folders. Hidden files are just like ordinary files in all other respects. You can choose whether a file is hidden or visible by changing its properties to designate it as hidden. Hidden files are generally used to reduce clutter, but they also make your system more secure to novice hackers because you can hide confidential files from other people, but you should not rely on hidden files as your only means of security or privacy.

2. **Hide protected Operating System Files** – These files are hidden by default, and you should keep them hidden. Hiding these files is usually a good idea, because it helps you avoid deleting them accidentally. But for some special purposes, you'll need to display these files temporarily.

3. **Show Encrypted Files or Folders in Colors** – This option could tell a hacker which files to target; therefore you might consider turning off this feature.

4. **Use Simple File Sharing** – Most security experts recommend turning off the Simple File Sharing in Windows 95, 98, 2000 and XP and that you use the standard File Sharing instead. (Simple Sharing is disabled by default in Windows Vista.) Simple File Sharing is used primarily in the Home editions of Windows XP and Windows Vista.

# Encrypting File System (EFS)

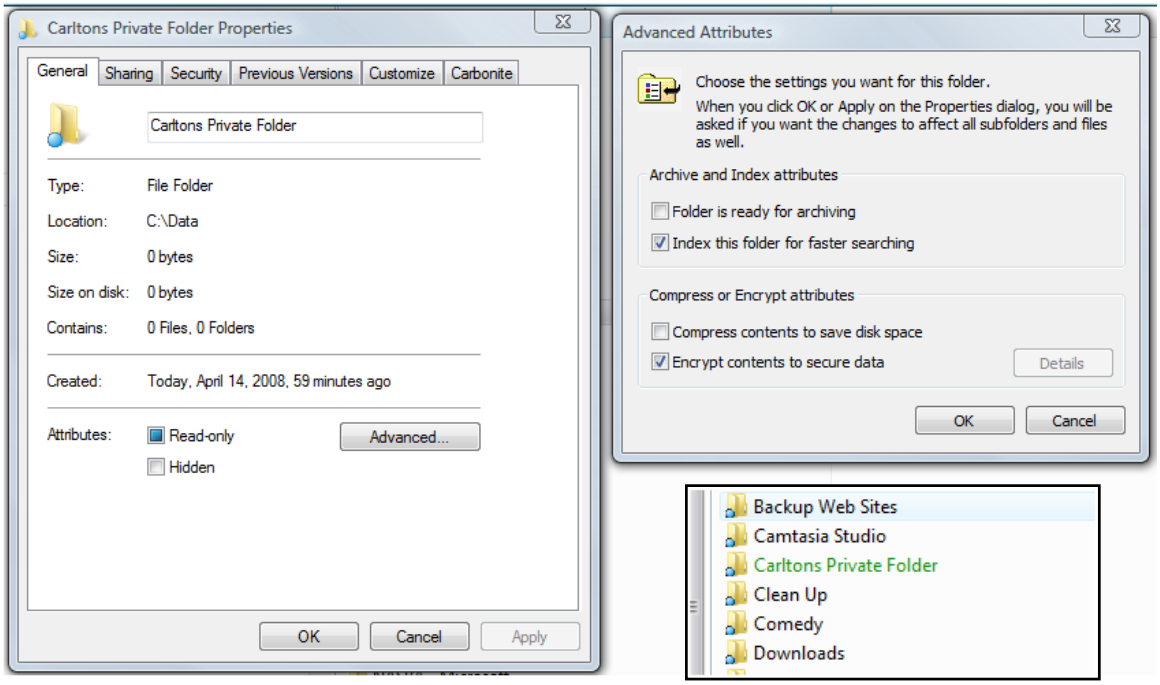
There's only one sure way to make your files truly confidential – you must encrypt them. The Encrypting File System (EFS) in most versions of Windows Vista, XP, and 2000 scrambles the contents of files and folders, making it impossible for others to read them (assuming a strong password is used and kept secret). Presented below are key points:

1. **Where is EFS? -** EFS is included in Windows Vista Business, Enterprise, and Ultimate; XP Pro; and Windows 2000; however, Windows XP Home lacks EFS, and Vista Home Premium, Vista Starter, and Vista Home Basic only allow decryption – this allows users to read encrypted files but not encrypt them.

2. **Must Use NTFS –** As mentioned above, to use EFS on a hard drive partition, that partition must first be formatted using the NTFS file system.

3. **Encrypt** - To encrypt a file or folder, right-click it in any folder and choose Properties - General tab – Advanced. Check “Encrypt contents to secure data”. If you're encrypting a folder, you'll be asked if you want to encrypt its files and subfolders, as well.

   Once encrypted, the files or folders will work like any others on your system; you don't have to use any special passwords to open or save them. However, other user accounts on the PC, and other PCs on the network, will not be able to view the file contents unless they are logged in to your account with your password.



**Tip -** You can add the “Encrypt” command to your right-click context menu using Tweak UI, a free PowerToy from Microsoft. To do this download Tweak UI for free, installed and launch Tweak UI, select Explorer in the left pane, and scroll to the option and check Show "Encrypt" on context menu.

4. **Color Coded -** Encrypted folders and files will appear in green text as an indication that the contents are encrypted. You can change this by opening Explorer and choosing Tools, Folder Options. Click the View tab, and in the Advanced Settings box, make sure that Show encrypted or compressed NTFS files in color is checked. Encrypted items will be shown in green and compressed ones blue. If you don't want others to see which files are encrypted or compressed, uncheck this option.

5. **Grant Permissions to Others –** You can grant users access to your encrypted files by user name. Do this by right-clicking a single encrypted file (not a folder or multiple files), and choose Properties. In the General tab, click Advanced, and next to 'Encrypt contents to secure data', choose Details. In the middle of that dialog box, click Add to open the Select User dialog, which lists others who have a certificate (a digital document that helps confirm authenticity) on your system. Users can acquire certificates in various ways, but one of the simplest is by encrypting one of their own documents. Select a trusted user and click OK.

6. **Disable Profiles Rather than Deleting Them** - Deleting a profile might prevent you from accessing an encrypted file. For example, if Steve goes on leave, you should disable rather than delete Steve's profile: To do this in XP, choose Start, Run, type lusrmgr.msc, and press Enter. In Vista, click Start and enter the same command in the Start Search field. Click the Users folder icon in the left pane and double-click Steve’s profile in the right pane. In the General tab, check “Account is disabled” and click OK; when Steve returns to work, simply reverse this procedure.

# System Restore

## Chapter 7

# System Restore

System Restore is a feature of Microsoft Windows XP and Vista that automatically saves a copy of important system settings (the registry) and files so that you can easily restore those settings if something goes wrong. System Restore creates a backup copy every day and every time you install new hardware or software.

If your computer starts functioning poorly, System Restore can be used to returns system settings and system files to the state they were in on an earlier date when the computer was working properly.


System Restore has saved my bacon many times, so I reserve as much disk space as possible for its restore points. *(Not everyone is a big restore point fan because it does not always work properly, but my experience has 100% great).* Comments follow:

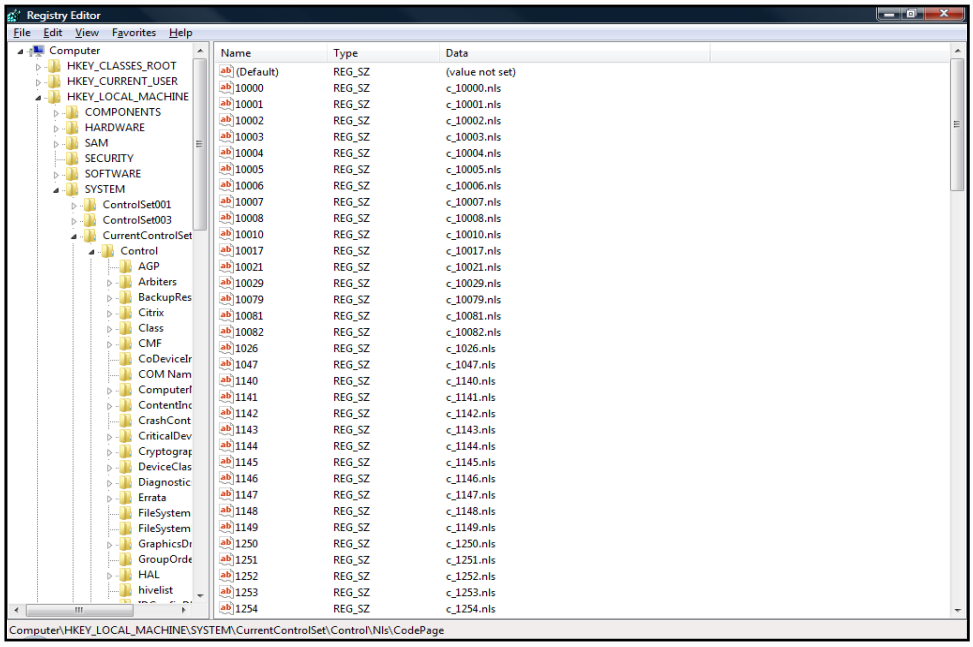
1. On Windows Vista computers, you need at least 300 megabytes (MB) of free space on each hard drive that has System Protection turned on.
2. System Restore might use up to 15 percent of the space on each disk.
3. As the amount of space fills up with restore points, System Restore will delete older restore points to make room for new ones.
4. System Restore will not run on disks smaller than 1 gigabyte (GB).
5. In Windows XP computers only, you can adjust the amount of disk space System Restore claims, right-click *My Computer* in Explorer or on the desktop and choose *Properties*.

Click the *System Restore* tab and select a drive whose storage settings you want to *change. Choose Settings, drag the slider to the desired level, and click OK twice.*

6. *Restore points are created automatically every day, and just before significant system events, such as the installation of a program or device driver. You can also create a restore point manually.*
7. *If you turn off System Protection (the feature that creates restore points) on a disk, all* restore points are deleted from that disk. When you turn System Protection back on, new restore points are created.
8. System Restore doesn't protect FAT32 and other FAT disks because FAT disks don't support the use of shadow copies. Shadow copies require the NTFS file system. In this version of Windows, System Restore uses shadow copies to create restore points. If you store system files on a FAT disk, you cannot use System Restore to undo changes.

## Understanding the Registry

The system registry is where Windows stores your computer settings and other information about how your computer runs. The registry is constantly changing as you install new programs and change settings in Control Panel and elsewhere. Here is what the registry looks like:




Ordinarily, you do not need to make changes directly to the registry because the registry contains complex system information that is vital to your computer, and an incorrect change to your computer's registry could render your computer inoperable. However, you can run the command REGEDIT to launch the registry and scroll its thousands of lines of content. Windows Restore Point takes snap shots of your registry which can be easily restored later if needed.

# Firewalls

# Chapter 8

## Firewalls

A firewall is a dedicated appliance, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.

The concept of needing a firewall first occurred with Clifford Stoll's discovery of German spies tampering with his system in 1988. That attack and others led programmers to apply filter rules to their network routers. The term “Firewall” was widely popularized when it was it was referenced in the movie war games.


## Routers and Firewalls Have Opposing Objectives

The whole point of the Internet is to allow for the free flow of information throughout the world. The whole point of the computer security is to prevent the free flow of information throughout the world. Given these two directly opposing objectives, it is easier to understand why air tight computer security is so elusive. The real trick is to allow authorized access to your systems, and to prevent unauthorized access. This is precisely what firewall devices can do for your organization.

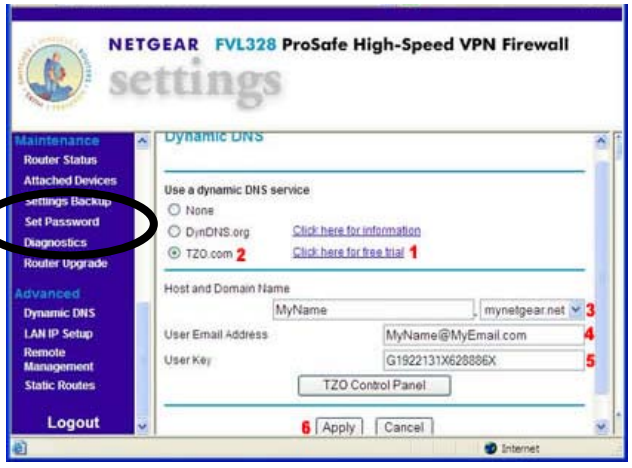
## Firewalls – Devices versus Software

Firewalls can be hardware devices, or software applications. Here are examples:


In my opinion, hardware device firewalls are better because they set up a defense against attack at the point where your Internet cable enters your building. Software based firewalls set up the defenses at the server (or worse at each computer), which potentially leaves your routers, printers, fax machines and other devices vulnerable. Because just one hardware based firewall can protect your entire organization's computer systems, I recommend a firewall device.

## Please Change the Firewall Password

The default login name and password for each firewall device is printed on the bottom of the firewall device – and is usually as follows: 168.192.0.1. Please login in and change the password.



## What Firewall Routers Do

Today's firewall devices provide several security features, as follows:

1. **Restrict Access** – Firewalls provide Network Access Rules that allow the administrator to block all traffic of a certain type, such as Internet Chat (IRC). Rules can be created to give Internet users access to a specific server on a LAN. Most importantly, firewalls provide absolute control of your ports, Java, ActiveX, Cookie, Proxy blocking, etc. The administrator can customize the firewall device to allow Java, ActiveX and cookies from trusted sites. When a proxy server is located on the WAN it is possible for LAN users pointing to this proxy server to circumvent content filtering.

2. **Hacker Attack Prevention** – Firewalls can inspect packets as they arrive to protect private LANs from Internet hackers and vandals by detecting and thwarting Denial of Service attacks such as Ping of Death, SYN Flood, LAND Attack, IP Spoofing, etc.

3. **Alerts** – Most firewall devices maintain a log of security events for later review. These events can also be sent to appropriate users via e-mail for immediate review, depending upon the severity of the event.

4. **Network Address Translation (NAT)** - Allows companies to use private addresses for better security.

5. **IP Address Management** - NAT also allows LANs to share low cost Internet accounts, such as xDSL or cable modems, where only one IP address is provided by the ISP.

A good comparison chart of Firewall features is available at this URL: http://en.wikipedia.org/wiki/Comparison_of_firewalls

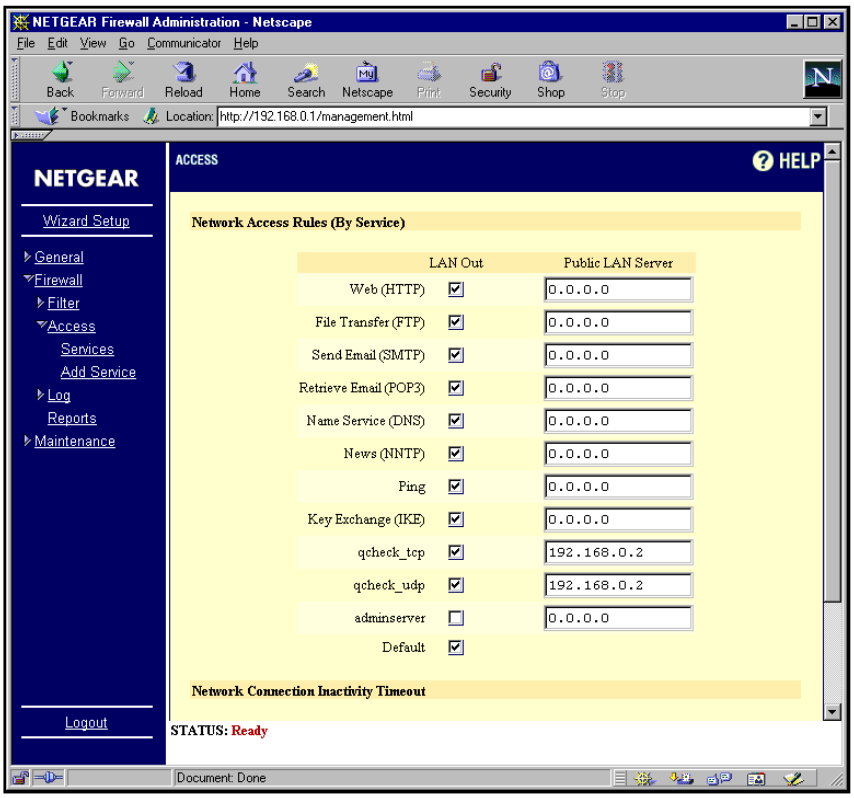

When shopping for a firewall appliance, make sure to select on that has been ICSA Certified. This internationally accepted certification means that the device has been subjected to a rigorous series of tests intended to expose vulnerabilities to attacks and intrusions. There are many firewalls in the marketplace ranging in price from $95 to $46,000.

# How Firewalls Filter Data

All data transmitted over the Internet has a sender's and recipients IP address embedded in each packet. As an example, consider this e-mail I received from Godiva Chocolates:

> Status: U
> Return-Path: <godiva@email.godiva.com>
> Received: from noehlo.host ([127.0.0.1]) by whmx-tenant.pas.sa.earthlink.net (EarthLink SMTP Server) with SMTP id 1jH4Y75i43NZFmB2; Wed, 2 Apr 2008 08:33:43 -0700 (PDT)
> Received: from mh.godiva.m0.net ([**209.11.164.74**]) by whmx-tenant.pas.sa.earthlink.net (EarthLink SMTP Server) with ESMTP id 1jH4Y73cx3NZFmB0 for <carlton@accountingsoftwareadvisor.com>; Wed, 2 Apr 2008 08:33:43 -0700 (PDT)

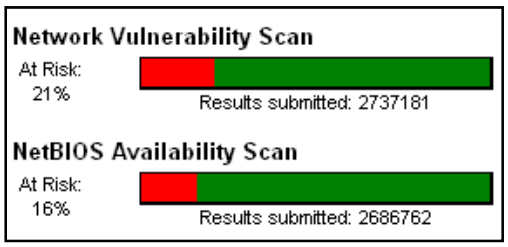
As you can see, the sender's IP address is embedded in the e-mail. With this information, I could simply instruct my firewall device to block all packets to and from this IP address (exclusive filtering). Likewise, I could also instruct my firewall device to block all packets except for those containing this IP address (inclusive filtering). The screen below shows where you would set up these rules on a NetGear Firewall device.



**You can Test Your Firewalls Effectiveness -** There are several web sites that you can visit that will test the vulnerability of your current internet connection and the effectiveness of your firewall device. One such web site offered by Symantec is located at the following URL:

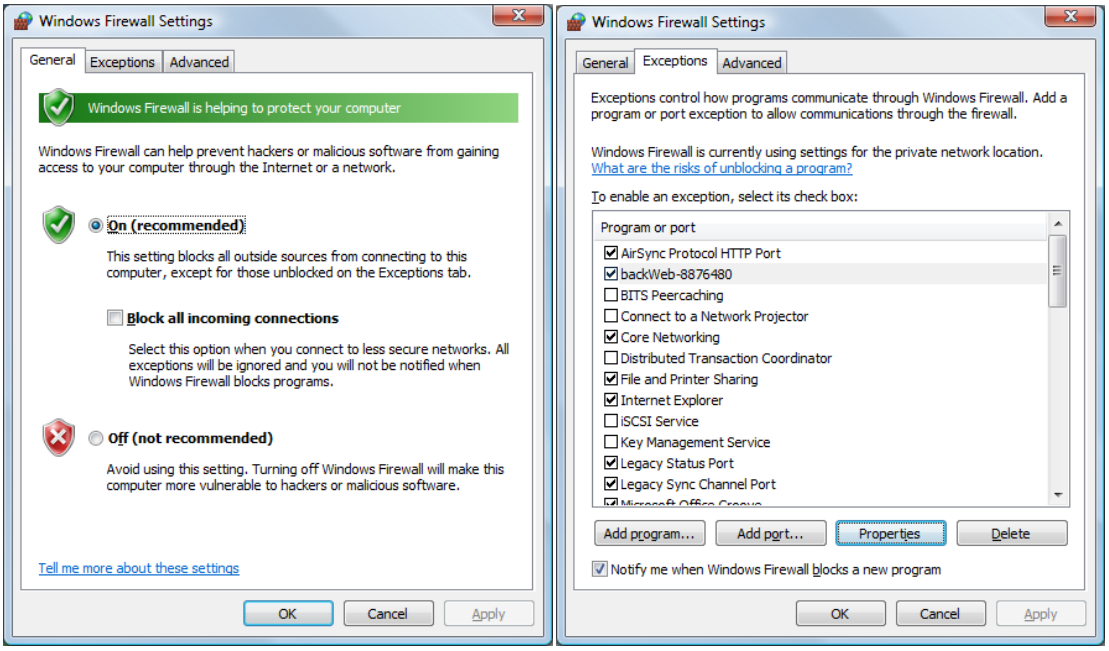
http://security.symantec.com/ssc/sc_ipcheck.asp?ax=1&langid=ie&venid=sym&plfid=23&pkj=OBQXESLHFEPGEVVSDUX

Symantec publishes the results of this online security testing and based on more than 2.5 million tests, 16% to 21% of all users are vulnerable to network and NetBIOS attacks via the internet. These results are shown below:




## Windows XP & Windows Vista Firewalls


Both Windows XP and Windows Vista have firewalls built right in, and they are excellent. To access the firewall settings, select Windows Firewall from Control Panel to display the following dialog boxes:



Following are a few points of interest regarding these firewall solutions.

1. Windows Firewall was first introduced as part of Windows XP Service Pack 2.

2. Every type of network connection, whether it is wired, wireless, VPN, or even FireWire, has the firewall enabled by default, with some built-in exceptions to allow connections from machines on the local network.

3. System administrators are able to configure Windows Firewall settings on a company-wide level.

4. XP's Windows Firewall cannot block outbound connections; it is only capable of blocking inbound ones.

5. Windows Firewall in Windows Vista significantly improves the firewall as follows:

    a. IPv6 connection filtering is now available.

    b. Outbound packet filtering is now available.

    c. Rules can be specified for source and destination IP addresses and port ranges.

    d. Rules can be configured for services by its service name chosen by a list, without needing to specify the full path file name.

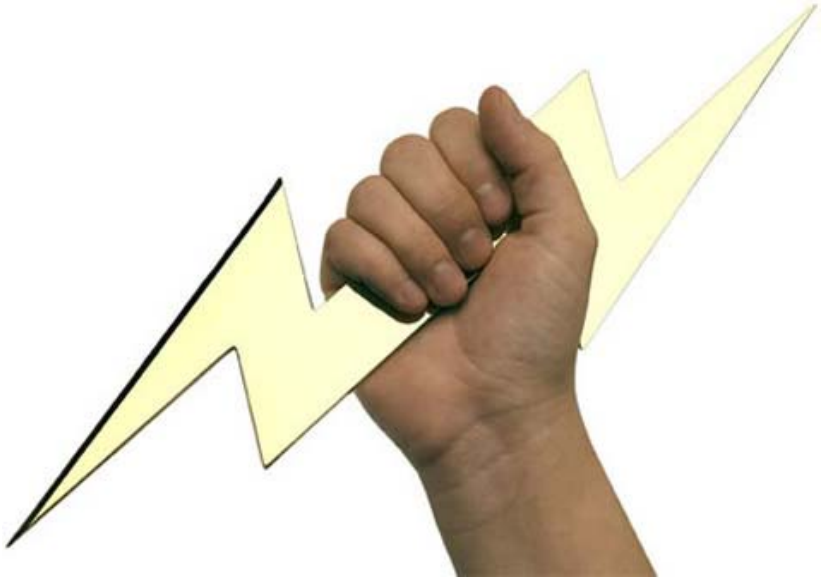
    e. IPsec is fully integrated, allowing connections to be allowed or denied based on security certificates, Kerberos authentication, etc.

    f. Encryption can also be required for any kind of connection.

    g. A new management console snap-in named Windows Firewall with Advanced Security provides access to many advanced options, and enables remote administration. This can be accessed via Start -> Control Panel -> Administrative Tools -> Windows Firewall with Advanced Security.

    h. Ability to have separate firewall profiles for when computers are domain-joined or connected to a private or public network.

If you have a firewall device, and use Windows built-in firewall solution, you do end up with redundant protection. This is fine; I see no significant problems or performance issues with running these two layers of firewall protection. In fact, the Windows firewall protection becomes important because it protects your computer from attacks from other employees or persons within your organization.



# Wireless Security

## Chapter 9

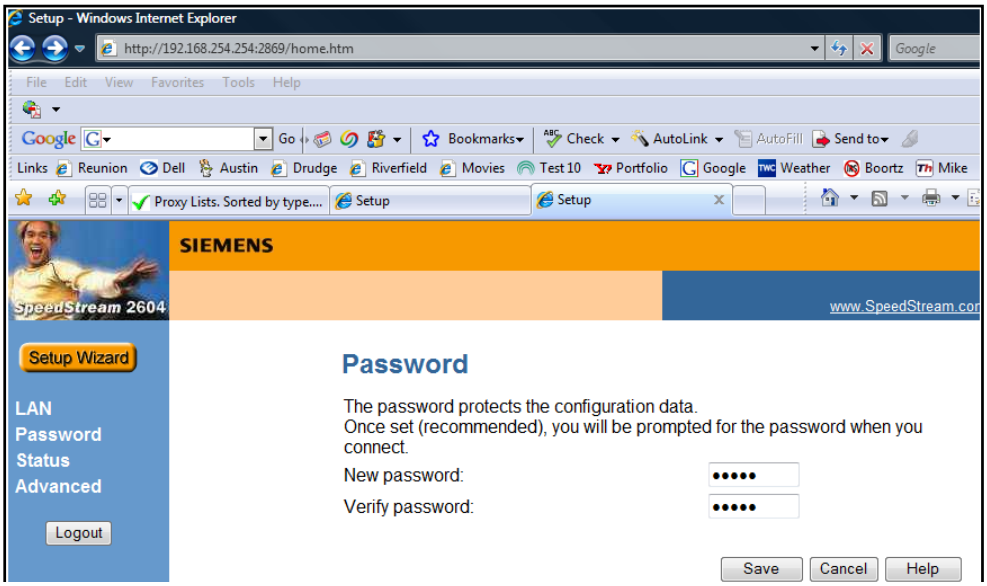
## Wireless Security

The use of a wireless device provides an invisible access point into your computer network in a range up to 300 feet radius from your wireless device. Hackers use empty tennis ball cans to build devices designed to detect and boost your signal, like the device shown below.

Many users setting up wireless home and small office networks rush through the job to get their Internet connectivity working as quickly as possible, but the fail to take the additional measures needed to properly lock down this new access point. The recommendations below summarize the steps you should take to improve the security of your home wireless network.

1. **Change Default Administrator Passwords (and Usernames)** – The first order of business is to log into your wireless device settings and change the default username and password. The default login name and password is usually "admin" and "password" – and all of the hackers out there know this. Therefore you should change these settings immediately. Here's how:

   a. *First, you must be connected to the wireless device with a physical wire (such as an Ethernet cable), you usually cannot do this wirelessly.*
   b. *Log In to the Network Router by typing the following into your browser: HTTP://192.168.0.1 or whatever IP address is printed on the bottom of the wireless device, if different.*
   c. *Navigate the menu to the Router's Change Password Page.*
   d. *Choose and Enter a New Password.*
   e. *Save the New Password.*




2. **Turn on WPA2 or WPA Encryption -** All Wi-Fi equipment supports some form of encryption scheme as follows:

   a. **WEP** (Wired Equivalent Privacy) – Found to have serious shortcomings in 2001.
   b. **WEP 2** – Also, found deficient, WEP2 mutated into TKIP.
   c. **WEPplus** – Lucent's attempt to correct WEP shortcomings, but this fell short.
   d. **Dynamic WEP** – 3COM's attempt to correct WEP shortcomings which fell short.
   e. **WPA** (Wi-Fi Protected Access) - the answer to WEP.
   f. **WPA2.0** – Better than WPA, but does not always work with older devices.
   g. **WPAPSK-TKIP** – Software driven
   h. **WPA2PSK-AES** – Hardware driven
   i. **WPA2PSK-TKIP** – Software driven

   Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read. Several encryption technologies exist for Wi-Fi today. Naturally you will want to pick the strongest form of encryption that works with your wireless network. However, the way these technologies work, all Wi-Fi devices on your network must share the identical encryption settings. Therefore you may need to find a "lowest common denominator" setting. Here's how you set up WPA:

   *j. First, verify that each computer is running Windows XP Service Pack 1 (SP1) or later.*

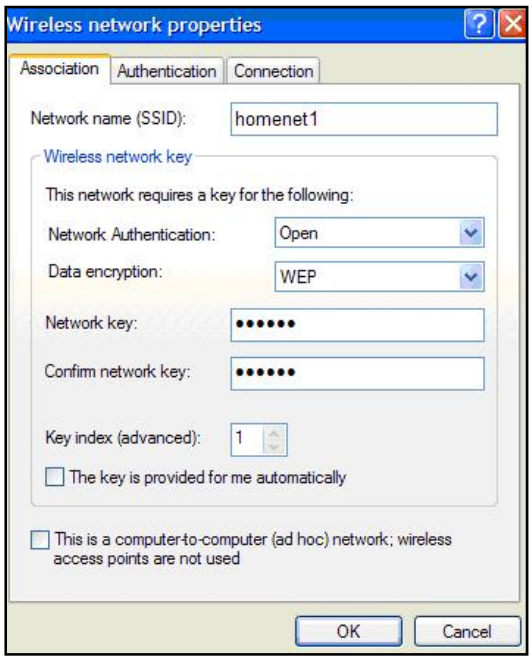
   *k. On each computer, verify that the client's network adapter is compatible with the **Wireless Zero Configuration (WZC) service**. (To do this, consult the adapter's product documentation, manufacturer's Web site, or appropriate customer*

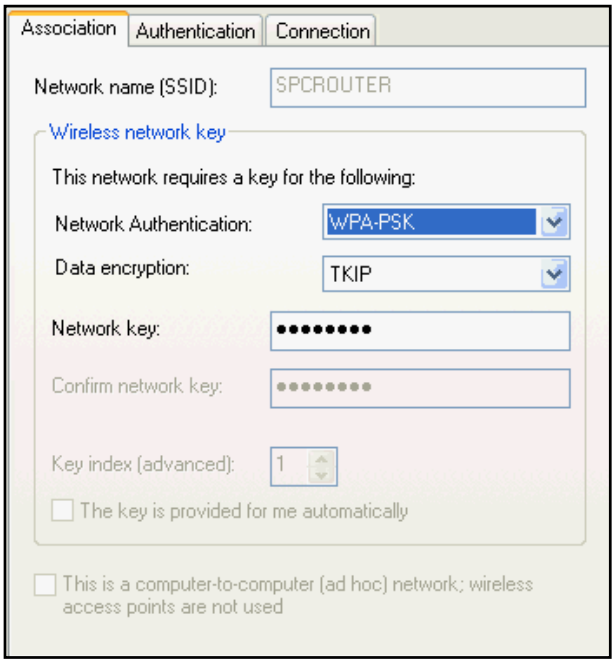
*service line for details. Upgrade the network adapter driver and configuration software to support WZC on clients where needed).*

*l. For each computer, download and install the [Windows XP Support Patch for Wi-Fi Protected Access](), walk through the installation dialog boxes and following the instructions.*

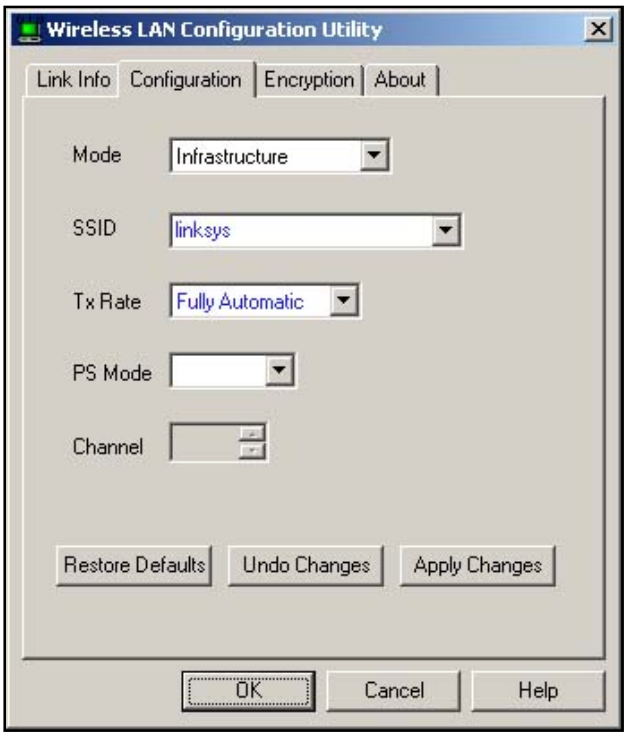
*m. Continue following the instructions and configure all **Wireless Access Points** (your wireless devices).*

*n. Continue following the instructions and configure all **Wireless Network Adapters** (your LAN cards).*



3. **Change the Default SSID -** Access points and routers all use a network name called the SSID. Manufacturers normally ship their products with the same SSID set. For example, the SSID for Linksys devices is normally "linksys." True, knowing the SSID does not by itself allow your neighbors to break into your network, but it is a start. More importantly, when someone finds a default SSID, they see it is a poorly configured network and are much more likely to attack it. Change the default SSID immediately when configuring wireless security on your network.




a. Log In to the Network Router
b. Navigate to the Router's Basic Wireless Settings Page
c. Choose and Enter a New SSID
d. Save the New SSID

4. **Enable MAC Address Filtering -** Each piece of Wi-Fi gear possesses a unique identifier called the physical address or MAC address. Routers keep track of the MAC addresses of all devices that connect to them. Many routers offer the owner an option to key in the MAC addresses of their home or small business equipment which restricts network connections to those devices only. Here's how:

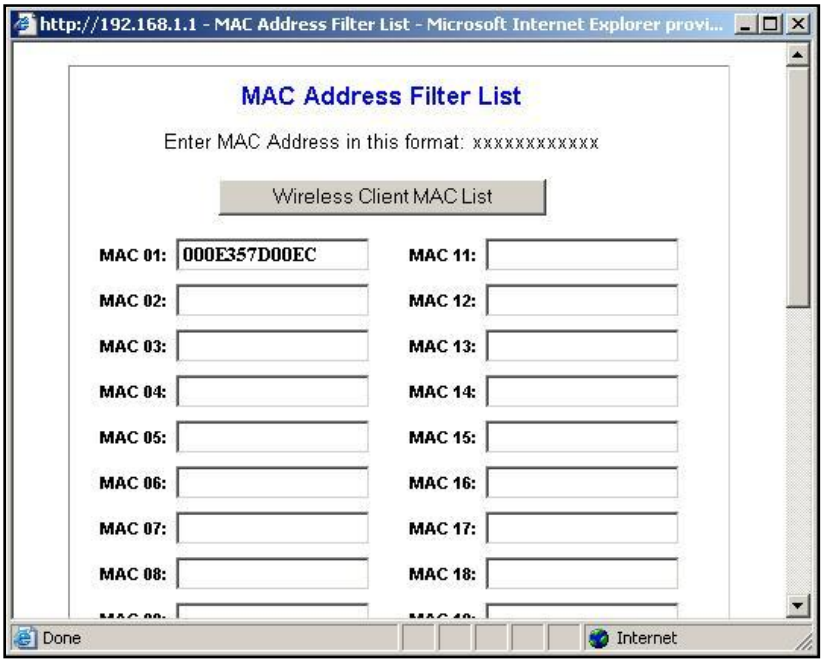
a. To set up MAC address filtering, first prepare a list of computers and devices that will be allowed to join the network.

b. Next, obtain the MAC addresses of each computer or device from its operating system or configuration utility.

c. Next enter those addresses into a configuration screen of the wireless router. An example screen is shown below.

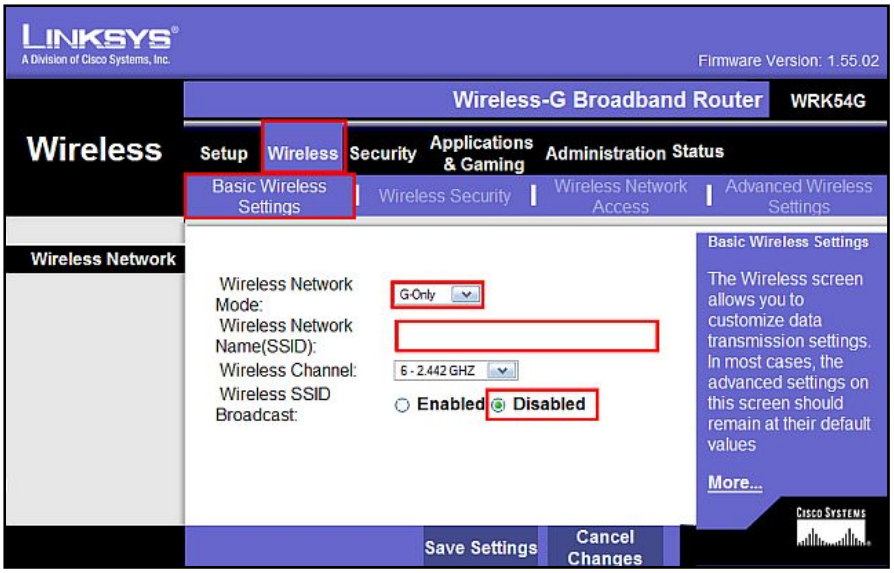
d. Finally, switch on the filtering option.

e. Once enabled, whenever the wireless router receives a request to join with the WLAN, it compares the MAC address of that client against the administrator's list. Clients on the list authenticate as normal; clients not on the list are denied any access to the WLAN.




(While this feature represents yet another obstacle/deterrent to hackers, there are many software programs available that enable hackers to defeat this measure by easily faking a MAC addresses.)

5. **Disable SSID Broadcast -** In Wi-Fi networking, the wireless router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses and mobile hotspots where Wi-Fi clients may roam in and out of range. In the home or small business, this roaming feature is probably unnecessary, and it increases the likelihood someone will try to log in to your home network. Fortunately, most Wi-Fi access points allow the SSID broadcast feature to be disabled by the network administrator. To do this simply log into your wireless router device, navigate to the SSID menu, and click the disable button as shown below.

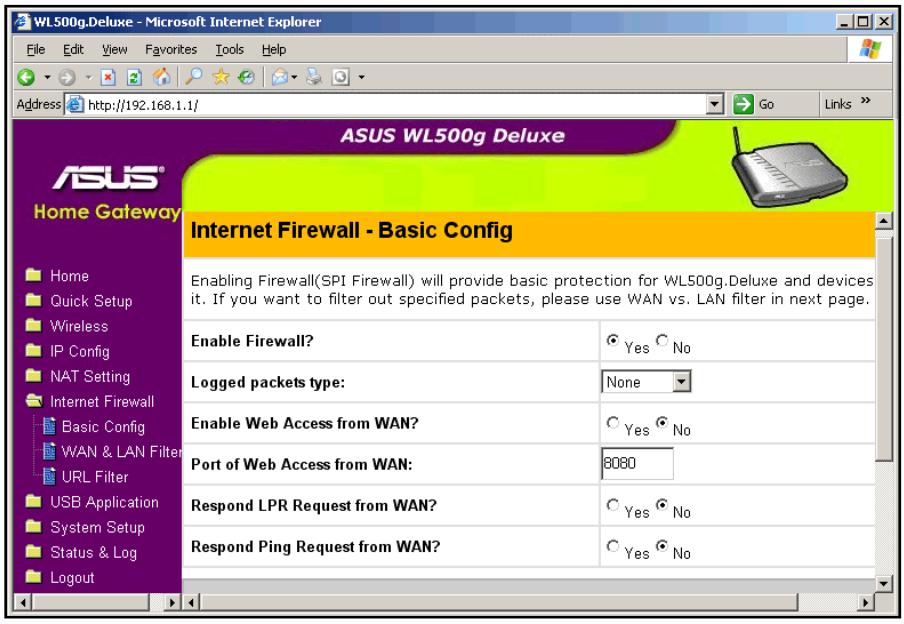



6. **Do Not Auto-Connect to Open Wi-Fi Networks -** Connecting to an open Wi-Fi network such as a free wireless hotspot or your neighbor's router exposes your computer to security risks. Although not normally enabled, most computers have a setting available allowing these connections to happen automatically without notifying you (the user). This setting should not be enabled except in temporary situations. Here's how:

   a. To verify whether automatic Wi-Fi connections are allowed, open Control Panel.
   b. Click the "Network Connections" option if it exists (otherwise first click "Network and Internet Connections" and then click "Network Connections.")
   c. Right-click "Wireless Network Connection" and choose "Properties."
   d. Click the "Wireless Networks" tab on the Properties page.
   e. Click the "Advanced" button.
   f. Find the "Automatically connect to non-preferred networks" setting. If checked, this setting is enabled, otherwise it is disabled.

7. **Assign Static IP Addresses to Devices -** Most home and small business networks use dynamic IP addresses because DHCP technology is easy to set up and use. Unfortunately, this convenience works to the advantage of network attackers, who can then obtain valid IP addresses from your network's DHCP pool. To be more secure, you may want to turn off DHCP on the router, set a fixed IP address range instead, then configure each connected device to match. Use a private IP address range (like 12.12.12.x) to prevent computers from being directly reached from the Internet. The specific procedures to follow will vary on the devices you are using, therefore you should refer to the user manual or web for detailed instructions for each device you have on your network.

8. **Enable Firewalls On Each Computer and the Router –** Wireless routers contain built-in firewall capability, but the option also exists to disable them. Ensure that your router's firewall is turned on. For extra protection, consider installing and running personal firewall software on each computer connected to the router. To do this simply log into your wireless router device, navigate to the Firewall menu, and click the Enable button as shown below.




9. **Position the Router or Access Point Safely -** Wi-Fi signals normally reach beyond the walls of a home or small office. A small amount of signal leakage outdoors is not a problem, but the further this signal reaches, the easier it is for others to detect and exploit. Wi-Fi signals often reach through neighboring homes and into streets, for example. When installing a wireless home network, the position of the access point or router determines its reach. Try to position these devices near the center of the home rather than near windows to minimize leakage.

10. **Turn Off the Network During Extended Periods of Non-Use -** The ultimate in wireless security measures, shutting down your network will most certainly prevent outside hackers from breaking in! While impractical to turn off and on the devices frequently, at least consider doing so during travel or extended periods offline. Computer disk drives have been known to suffer from power cycle wear-and-tear, but this is a secondary concern for broadband modems and routers.

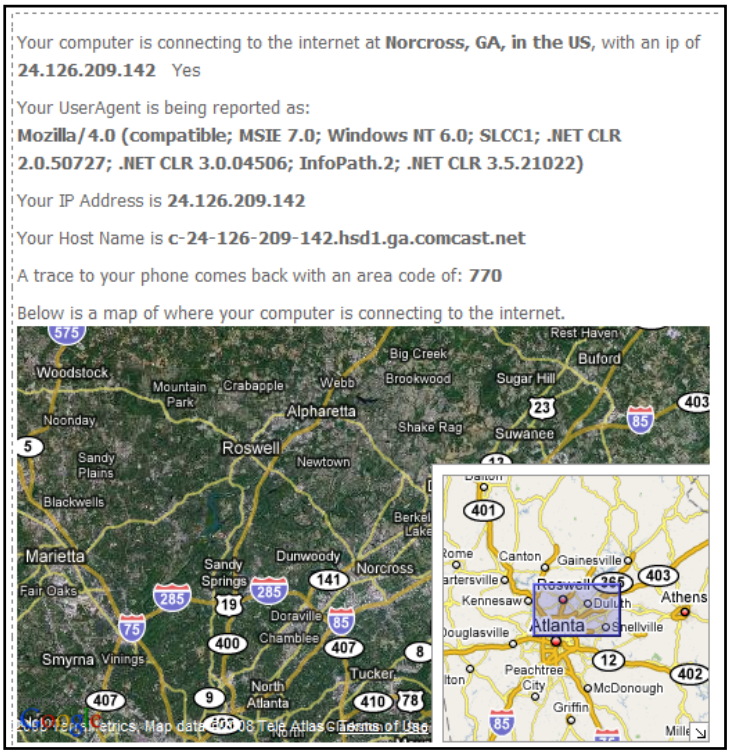
If you own a wireless router but are only using it wired (Ethernet) connections, you can also sometimes turn off Wi-Fi on a broadband router without powering down the entire network.

# Checking the Security of Your PC

## Chapter 10

1. **Firewall Test -** A firewall test should be conducted often and is easy to do. This test will check your computer for ports that are commonly left open. Open ports could allow your computer to be compromised. As an example, you could run a firewall test in less than 10 seconds at: http://www.auditmypc.com/firewall-test.asp. This firewall test will also check for open ports known to be used by Viruses and Trojans.

2. **Anonymous Surfing Test -** Anonymous surfing is a key step to staying safe online. It tested my computer at http://www.auditmypc.com/anonymous-surfing.asp, and immediately it showed me the following:




This means that a web site or other person can tell where I am located (approximately).


**Hide Your IP -** To thwart this possibility, I would need to hide my IP address using an anonymous proxy. Be very careful though as not all proxy servers do as they claim. In fact, many junk proxy servers give people a false sense of security or worse, and instead record everything you do in hopes to score a password or two! You can hide your IP with many products including this one:

The product claims to provide the following benefits:

1. **Easily Conceal Your IP Address** - Just click "Hide IP" and your IP is instantly hidden! Other people see a fake IP, which is not associated with your real IP.

2. **Anonymous Web Surfing** - Protect your privacy and cover your tracks! Select from one of our many fake proxy IP addresses for totally anonymous browsing.

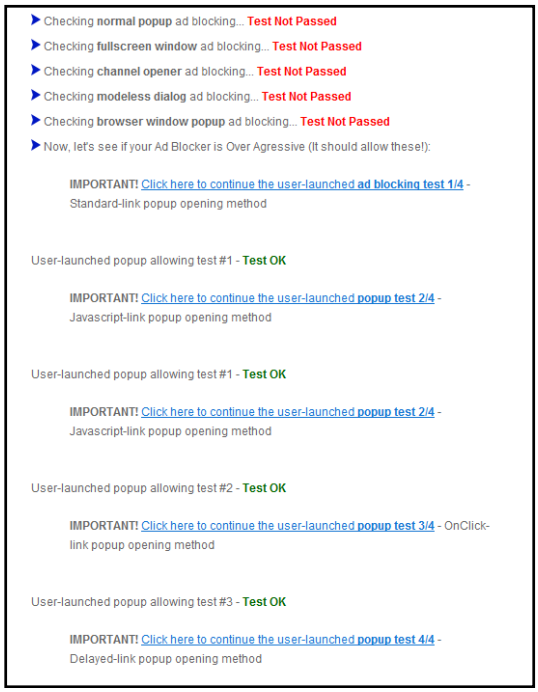
3. **Works with many Applications** - Hide My IP 2007 works with all major browsers and dozens of instant messengers, E-mail clients, and games.

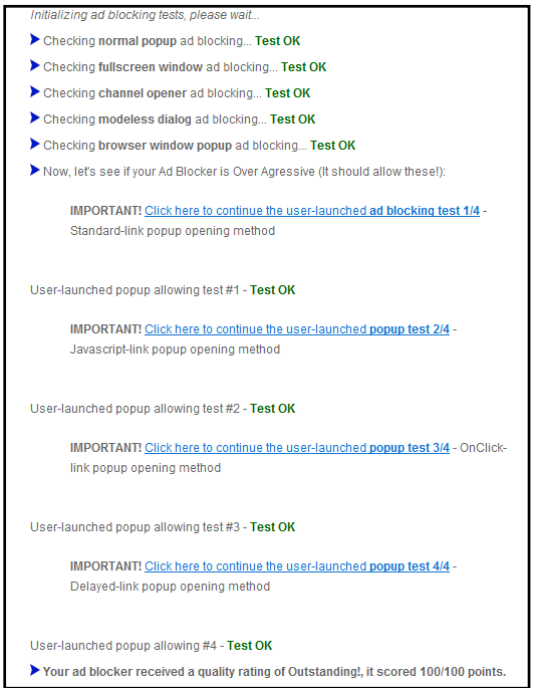
4. **Stop Hackers** - Identity thieves can potentially use your IP addresses to compromise your computer by installing key loggers, Trojans, and other tools.

5. **Send Anonymous Emails** - Hide your IP in E-mail headers. Supports Webmail services like Yahoo, Hotmail, and GMail. Mail clients supported with a Premium account include Outlook, Outlook Express, and Eudora.

6. **Un-ban Yourself From Forums, Blogs, Etc...** - By faking your IP you can often access many sites you were banned from. Combine with Cookie Crumble for the most effectiveness.

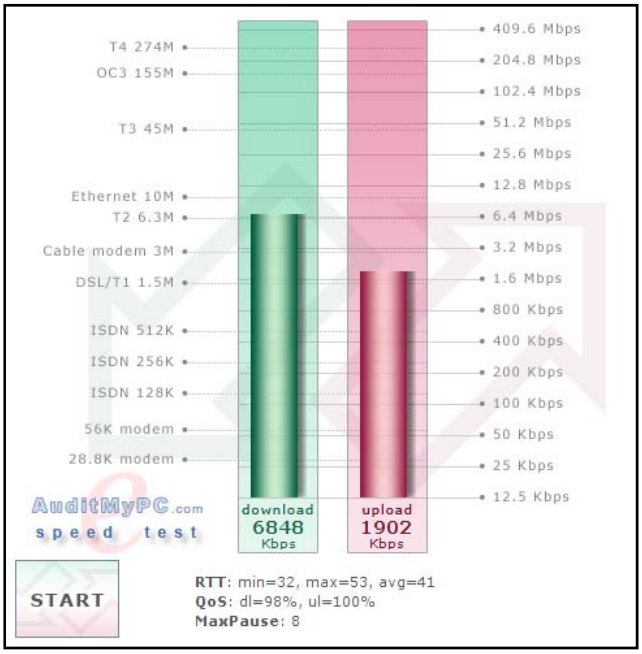
3. **Popup Test –** At a minimum, unwanted pop up ads steal time and provide a distraction. Popup Test to help you verify your ad blocking software is really capable of preventing pop up ads. I tested my computer for pop ups at http://www.auditmypc.com/freescan/popup/popup-test.asp. I did not have my pop up blocker turned on, and therefore I failed the test. Then I turned on the Internet Explorer Pop-Up Blocker and re-ran the test. The results before and after were as follows:



After turning on the standard Internet Explorer Pop Up Blocker, I passed the Pop up test with flying colors.

4. **Internet Speed Test –** A slow Internet connection can steal your productivity. Therefore you should conduct an Internet Speed Test for Broadband, Cable, Satellite and DSL Modems that helps determine your true bandwidth. I tested my speed here: http://www.auditmypc.com/internet-speed-test.asp. Here are the results:




This test provides you with your true speed, rather than the speed claimed by your provider. This will help you identify the problem in the event that you are not getting all the speed you are paying for. I recommend Cable at a minimum; in my opinion DSL is too slow and should be used when it is the only option.

# Online Security Tests

## Chapter 11

## Online Security Tests

ShieldsUp! - Port Authority Edition grc.com
*Internet Vulnerability Profiling, Gibson Research Corporation* - by Steve Gibson. [Free service] Checks the security of your computer's Internet connection by performing queries and probing common port addresses. A report is issued on your hacker vulnerability. "Port Authority" is the second-generation ShieldsUP!!

Broadband Tests and Tools www.broadbandreports.com/tools
*BroadbandReports.com* [Free service (limited use); Fee required for unlimited use] Internet speed tests, tweak test, line quality, line monitor, whois, doctor ping, router watch, and more.

BrowserSpy gemal.dk/browserspy
[Free service] Shows you what detailed information is revealed about you and your browser - version, what it supports, JavaScript, Java, plug-ins, components, bandwidth, language, screen, hardware, IP, cookies, web server, and more.

GFI Email Security Testing Zone www.gfi.com/emailsecuritytest
*GFI Software Ltd* [Free service] Find out how secure your e-mail system is by doing a vulnerability check.

Hacker Whacker www.hackerwhacker.com
[First test is free; Subscription fee applies on subsequent scans] See your computer the way hackers do. The following issues are addressed: Are there strangers in your computer? Could your web server be hijacked? Free security scan. Has your network been broken into? Are you secure? Are hackers targeting you? Want to test your firewall? Also contains a listing of current news articles on hacks, and a listing of links to other security sites.

PC Flank www.pcflank.com
[Free service] Test Your System - Choose from Quick Test, Stealth Test, Browser Test, Trojans Test, Advanced Port Scanner, and Exploits Test. (Kudos to the webmaster for great site design!)

PC Pitstop www.pcpitstop.com
[Free service] Internet Security test, Internet Ping test, Spyware check, In-memory virus check, bandwidth tests, assorted benchmarks, and more.

Qualys' Free Browser Checkup browsercheck.qualys.com
*Qualys* [Free service] A series of audits designed to test and fix your browser's security vulnerabilities. Supports only Microsoft Internet Explorer, and you must have cookies enabled.

Privacy.net privacy.net/analyze
*The Consumer Information Organization* [Free service] Privacy analysis of your Internet connection - performs tests on information that is collected about you when visiting a web site with explanations of what each test is and how it is performed.

ScannerX scannerX.com
[Initial assessment is free; Choose from a variety of plans - subscription fee applies] Vulnerability assessment services provide detailed testing, reporting and fixes.

Secunia www.secunia.com
[Free service] Online services include browser checker, online anti-virus, and vulnerability scanner.

Security Space www.securityspace.com
*E-soft Inc.* [Free "Basic Audit"; First "Desktop Audit" is free, subscription fee applies on subsequent tests] "Basic Audit" - Our classic port scan - scans 1500+ known service ports looking for services hackers might use to get in. "Desktop Audit" - A comprehensive suite of 797 vulnerability tests to learn if your system's security is at risk.

Symantec Security Check securityresponse.symantec.com Click on "check for security risks".
*Symantec* [Free service] A service designed to help you understand your computer's exposure to online security intrusions and virus threats.

Trend Micro Housecall housecall.trendmicro.com Click on "check for security risks".
*Trend Micro* [Free service] An online virus scanning service.

**File Authentication & Leak Tests:**

FireHole keir.net/firehole.html
*Robin Keir* [Freeware] Another tool for testing the outbound detection of personal firewalls. For use with Netscape and Internet Explorer.

LeakTest Firewall Leakage Tester grc.com/lt/leaktest.htm
*Internet Connection Security for Windows Users, Gibson Research Corporation* - by Steve Gibson. [Freeware] This small utility will test for vulnerabilities that might allow a malicious program to bypass your software firewall.

TooLeaky tooleaky.zensoft.com
*Bob Sundling* [Freeware] Test your firewall with a program that can defeat the outbound detection of personal firewalls. For use with Internet Explorer.

# Windows Security

## User Accounts & Security Groups

# Chapter 12

## User Accounts & Security Groups

8. **The Login Screen** - When logging into Windows, you are greeted by the Welcome screen. You must log in as a user to continue.

9. **No Security in W95 & W98 -** In Windows 95 and Windows 98, there was no security because you could simply hit the ESCAPE to continue.

10. **User Accounts Now Required -** Windows XP and Windows Vista force you to create a user account; you can create up to five user accounts.

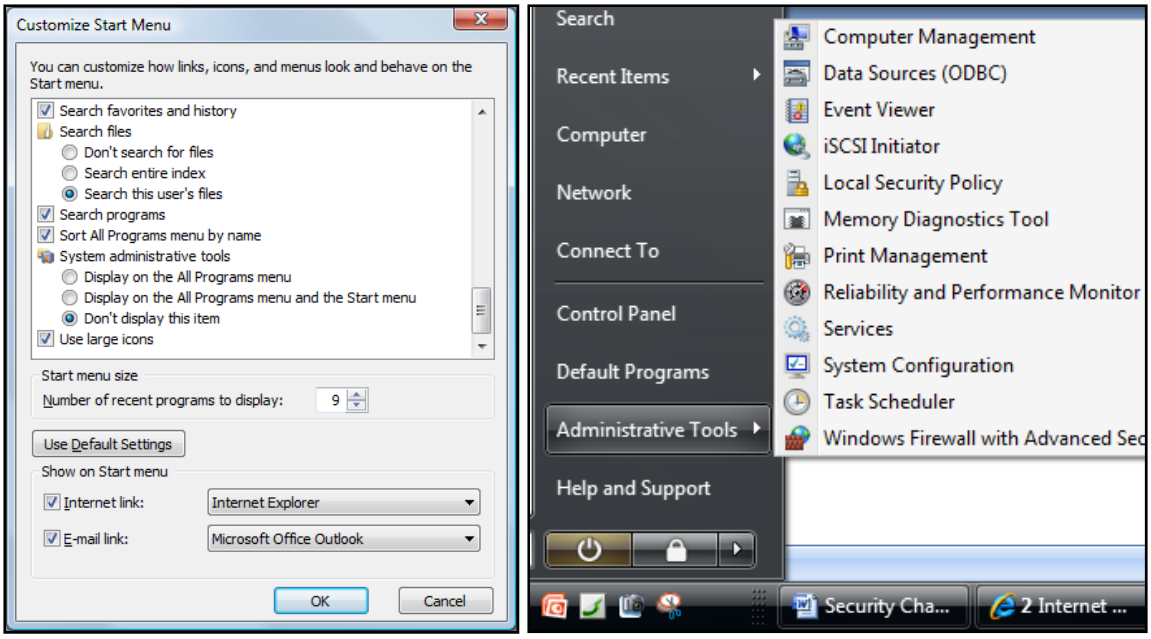

11. **Accessing User Accounts** – The **Control Panel - User Accounts** option allows you to see the user accounts that are allowed to log in; however there are other hidden user accounts used by the operating system and applications that are not shown.

12. **Limiting User Accounts -** The more user accounts you have, the more targets a hacker has. Therefore, you might consider limiting the number of user accounts using the hidden Administrative Tools.

13. **Making Administrative Tools Visible -** To do this:

    a. Right-Click the Start Button
    b. Select Properties
    c. Click the Start Menu Tab
    d. Click the Customize Button
    e. Click the Advanced Tab (in Windows XP only, Vista users simply scroll down)
    f. Select Option to Display Administrative Tools

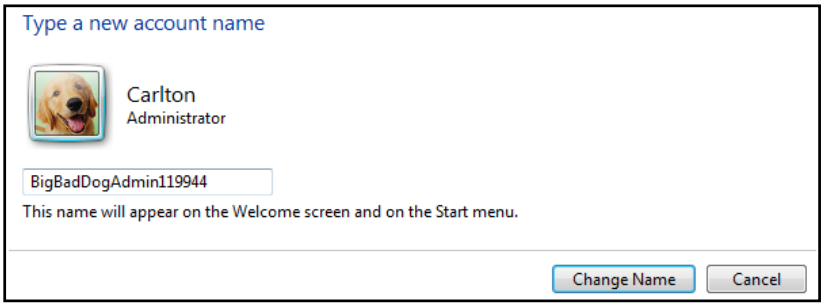
    The dialog box and resulting administrative tools are shown below.




14. **Disable the Guest Account in W95, W98, W2000 and Vista** – Most security experts advise you to disable the Guest account because it serves no real world purpose, it has no password by default, and hackers like to target the guest account. In Windows 95, 98, 2000, & Vista, disabling the Guest account is easily accomplished via a button selection in Control Panel's User Account dialog box.

15. **Password Protect the Guest Account in Windows XP** - In Windows XP, turning off the Guest Account only hides it from the log in screen - it still remains active behind the scenes because it is necessary for sharing resources on a network. Therefore rather than turning off the Guest Account, you should apply a strong password. Creating a password for the Guest account in Windows XP is easy, but it is also not an easy task in Windows XP Home. When you open the User Accounts console from the Control Panel in Windows XP Home and select the Guest account, Create a Password is not one of the available options. To create a password for the Guest account in Windows XP Home, you will need to open a command line window (click Start | All Programs | Accessories | Command Prompt). Enter the following: net user guest <password>. Leave off the brackets and simply type the password you want to assign at the end of the command line and press Enter. Oddly, now that you have created a password for the Guest account, the options for changing or removing the password will now appear in the User Accounts console.

16. **Rename the Administrator Account** – To hack into your computer, a hacker needs to know both the user name and the password. Everyone already knows the name of the administrator account. By changing the name of the administrator account, you compound the hacker's efforts. This is easy – just log into Windows as the "Administrator", go to "Control Panel – User Accounts", Choose the "Change Name" option, and enter a new name as shown below:

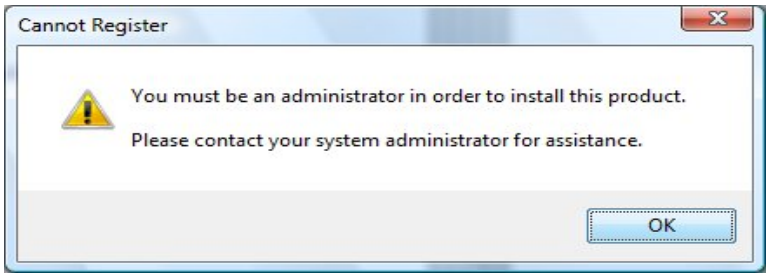



17. **Security Groups** – Just as you can create user accounts, you can also create security groups. The default groups that are included in the Windows are as follows:

    a. **Administrators** – Can do everything
    b. **Users** – Can use system, but can't install or change system
    c. **Power Users** – Grants some power to install and configure the system
    d. **Guests** – Limited access, can see shared folders and printers
    e. **Help Services** – Allows support technicians to connect to your computer
    f. **Backup Operators** – Can back up and restore files
    g. **Replicators** – Can copy files
    h. **Network Configuration Operators** – Add, change or delete network connections
    i. **Remote Desktop Users** – Can connect remotely

    Groups are helpful in larger organizations because the administrator can simply set up a few groups, and then assign users to those security groups. They will automatically inherent the security rights of the group they belong to. The use of security groups is considered to be faster and more accurate. (Security groups are not available in the Home editions of Windows XP and Windows Vista).

18. **Administrator Rights Required in Vista** – Windows Vista allow users to be standard users or administrators. Beginning in Windows Vista, you must be logged in as an administrator to accomplish many things such as install software or to change computer settings. This can be frustrating because standard users will encounter this obstacle frequently, and they will need to log in as an administrator frequently in order to manage their computer system. This is actually a great security measure, but it frustrates standard users and you should be aware of this problem. Following is an example screen that standard users will see frequently.



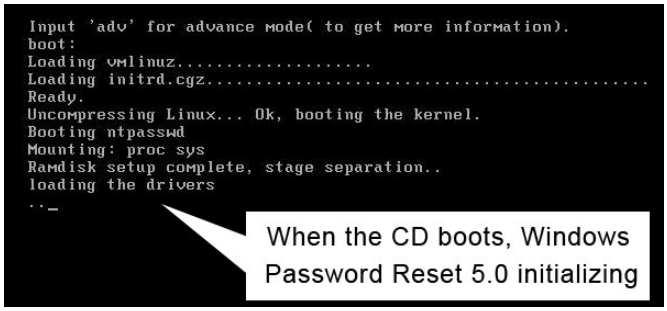
## Beware the Hacker Tools

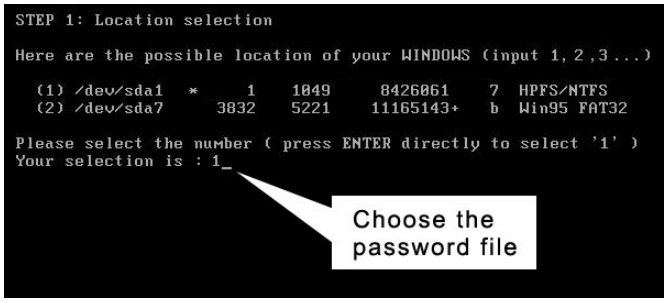
There are a multitude of hacker tools available for circumventing the user accounts and passwords. Microsoft continually releases patches to shut down these tools, but the companies that make these tools keep finding new ways to circumvent them.

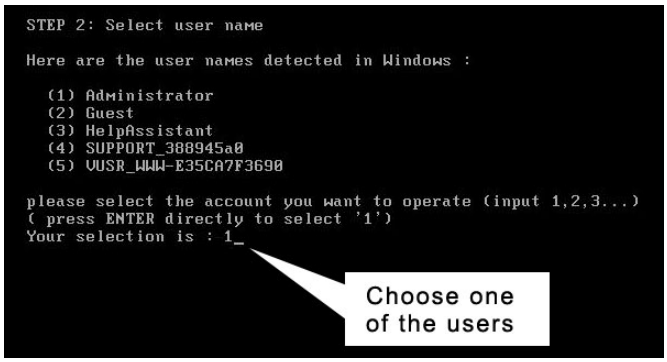

**Windows Password Reset 5.0** is just one of many similar programs designed for resetting local administrator and user passwords on any Windows system. The company claims that if you have forgotten your password, or are locked out, or you do not have access to the password of the system, you can easily get back in. Key features claimed:

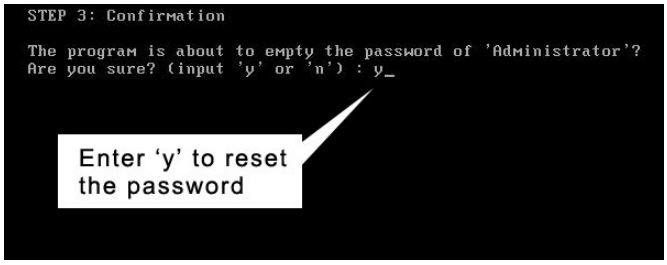
1. 100% recovery rate
2. Very easy to use(3 steps only), with complete screenshots
3. No other installation required
4. Supports FAT16, FAT32, NTFS, NTFS5 file systems
5. Supports large hard disk drives (even greater than 200GB)
6. Supports IDE ATA SATA & SCSI hard disk drives
7. Supports Windows XP, XP+SP2, 2003, 2000, NT, Windows XP Professional x64 Edition (64-bit), Windows Server 2003 x64
8. Edition (64-bit) Operating Systems, Windows VISTA, Windows VISTA(64-bit) & Windows Server 2008
9. All passwords are reset instantly
10. 100% Money back guarantee

Presented below are a series of screens that show how the product works.




# Windows Security

## Password Protected Screen Savers

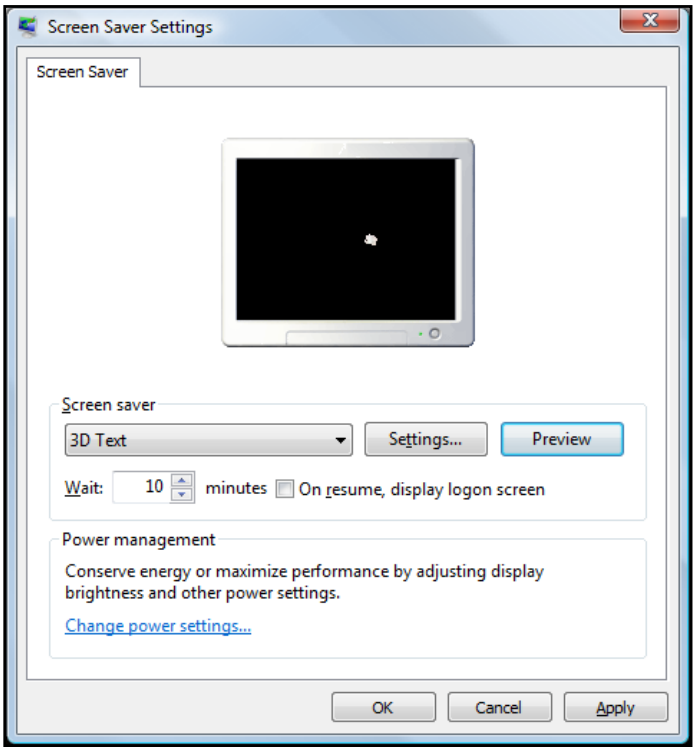
## Chapter 13

## Windows Screen Savers

Originally, a screensaver was a type of computer program designed to prevent a problem known as "Phosphor burn-in" on CRT and plasma computer monitors by blanking the screen or filling it with moving images when the computer was not in use. Today, newer flat panel LCDs monitors do not need a screen saver protection, but screen savers are actually very useful for security purposes.

> *(The first screensaver (written for the original IBM PC by John Socha) was published in December 1983 issue of the Softalk magazine. It simply blanked the screen after three minutes of inactivity.)*

Today most Windows screen savers can be configured to ask users for a password before permitting the user to resume work. To do this, right click the Windows Desktop and select personalize, Screen Saver. Indicate the number of minutes of inactivity desired before the screen saver kicks in, and check the box titled “On Resume, Display Logon Screen”.

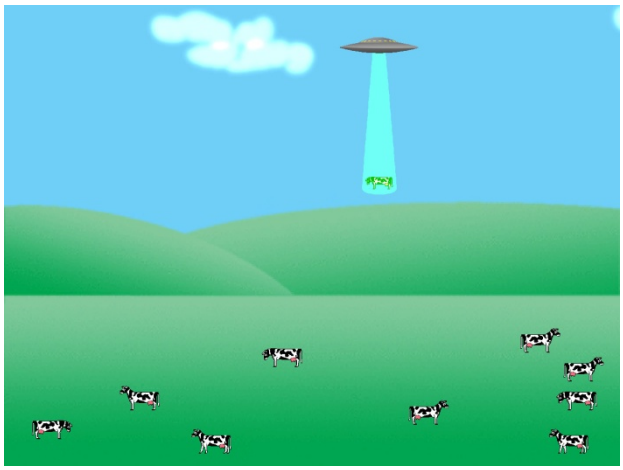



Now your computer screen will revert to the screen saver and will become locked until the proper password is applied. Of course if the hacker reboots your computer, they will encounter the Windows logon screen.

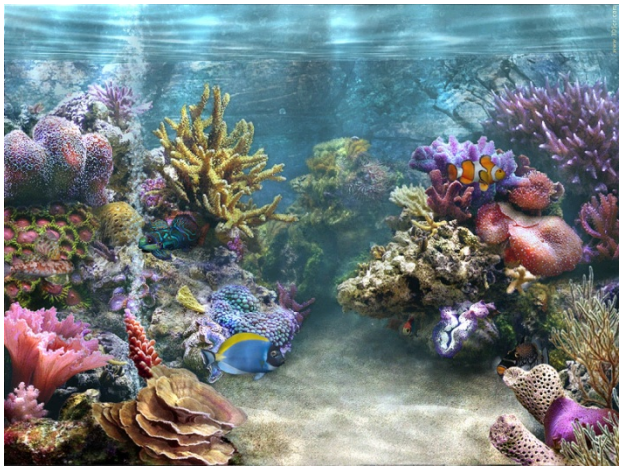
Trips to the bathroom do happen, brief departures from your desk do become extended. For these reasons and many more, it makes good sense to apply a password Protected screen saver to your computer.


There are many great screen savers out there. Windows allows you to turn your photos into a screen saver. PhotoImpression allows you to create a slide show screen saver set to music. There are also many clever screen savers out there like these:

Windows Vista Bubbles



Beaming Cows



Aquariums

Noah's Ark

Fancy Cars

Beautiful Scenery

Exciting

Cute Animals

Funny

Sports

Be careful not to download a screen saver from an un-trusted web site – you could be inadvertently downloading a virus, spam, or Trojan horse onto your computer.


# Pornography

## Chapter 14

# Pornography

If you supply your employees with a computer and Internet access, and they use that equipment view pornography at work, and another employees see it – are you liable? The answer is yes, you most are certainly liable unless you have taken reasonable measures to protect employees from pornography. Even if litigation is not an issue, pornography can steal employee productivity and pornographic web sites are often a source of spyware, malware and viruses. Presented below is a list of possible measures you should take in your organization to block pornography.

1. **Written Policy** – Provide all employees with a written policy explaining that the accessing or viewing pornography with company computers, company e-mail or during company hours or during company activities is forbidden. This provides notice. (See the chapter on documents for an example.)

2. **Signed Agreement** – Ask employees to sign a contract in which they agree not to access or view pornography using company computers, company e-amil or during company hours or during company activities. This may help shield you from liability. (See the chapter on documents for an example.)

3. **Require Safe Searches Only** – Most search tools such as Google, Yahoo! And MSN provide an option which filters 99.99% of all pornography from the search results. You should require your employees to always leave the safe Search setting to on.

4. **Plain View** – You might require all employees to always work in plain view of others with doors opened and computer screens visible to passerby's as a deterrent, unless conducting a confidential meeting.

5. **Use A Router Based Content Filter** – Consider using a router based content filter to block pornography. For example, the ContentProtect Security Appliance monitors everything going in and out on a real time basis. Features include:

    a. ***Dynamic Content Filtering:*** Identifies and blocks objectionable web material.
    b. ***Bandwidth Management:*** Monitors bandwidth usage to ensure good performance.
    c. ***Spyware:*** Tracks spyware to see who's catching it, and neutralizes the threat.
    d. ***Slow Internet:*** Discover the problem, down to the individual user.
    e. ***Bandwidth Abuse:*** See who's hogging it, and what they're using it for.
    f. ***Web Activity:*** See who's visiting what sites when, and what they're doing on them.
    g. ***Peer-to-Peer:*** Find out what P2P apps are doing to your network.
    h. ***Instant Messaging:*** Know who's talking, and what they're saying.
    i. ***Viruses:*** Prevent viruses, including those in web-based emails.
    j. ***Anonymous Proxies:*** Prevent users from bypassing your filters and safeguards

6. **Check Bread Crumbs** – Use the chapter on Bread Crumbs to randomly check employee computers for inappropriate pornographic activity.

7. **Monitor Employee E-Mails** – By law, companies have the right to read employee e-mails sent or received on company provided computers or at the company's place of business – even personal e-mails. You should random check e-mails to give notice to employees that their systems are being checked, and pornographic activity will not be tolerated.

8. **Employee Training** – Make employees aware of all aspects related to pornography. For example, simply viewing a pornographic web site – even for a moment - will leave pornographic images in the browser history files. If just one of those pictures is of an under-aged child, then you could be legally charged as a pedophile (I think). (The Child Pornography Prevention Act of 1996 was struck down in 2002 for being overly broad.)

What would a chapter on pornography be without a picture of some naked blonde chicks or a nude thumbnail of Brad Pitt? Here you go:

Naked Blonde Chicks

Nude Thumbnail of Brad Pitt

**(Yes, this is a joke) (Yes, I know its not that funny)**

**Pornography & Inappropriate Web Access -** The 1999 CSI/FBI Computer Crime and Security Survey indicates that ninety-seven percent (97%) of companies report that their employees abused Internet access. According to the Saratoga Institute of Human Resources, *"more than 60 percent of American company employee have been disciplined—and more than 30 percent have been terminated for inappropriate use of the Internet.*" Common abuses include accessing pornography, chatting online, gaming, investing, or shopping at work. According to some statistics, employees spend more than one hour per workday surfing the Web for personal reasons. The Institute estimates that *"a company with 1,000 employees who use company Internet access one*

*hour per day for personal surfing can cost a company upwards of $35 million each year in lost productivity"*.

Recently, higher bandwidth internet activities such as Internet Radio, PointCast, stock tickers, popup ads, music downloads, etc. are eating into corporate bandwidth. This significant increase in traffic can adversely affect other business operations such as e-mail, printing, data saving and retrieval, or operating business applications.

At a minimum, here are some steps that you can take:

1) Establish and publish a written policy that states:
    a. The company's access to the Internet and company e-mail should be used in much the same way that the business telephone is used - brief personal usage infrequently is OK, but is not to be abused.
    b. Visiting pornography web sites is strictly prohibited.
    c. Visiting web sites of terrorists, gangs, hate groups, etc. with company equipment is strictly prohibited.
    d. Employees should be aware of the Internet's unique ability to distract them from their normal work duties, accordingly, employees should learn to recognize and avoid this problem.
    e. Employees are prohibited from playing games on the Internet.
    f. Employees are prohibited from downloading any file that is not business related.
    g. Employees should use caution when providing company information across the web.
    h. Other restrictions you feel are necessary.
2) Consider activating Content Advisor on all employee computers, thereby limiting access to rated pornographic sites.
3) Consider installing a blocking program to block selected sites.
4) Routinely check employee computers at random - history files, e-mail, cookies folder, links, and GIFs.
5) Establish and use e-mail filtering rules to cut down on the amount of junk mail received by employees.

**Conclusion**

In conclusion, it should be obvious to anyone that the dangers are real – your computer systems are vulnerable in many ways. However, there are also a wide range of well proven and affordable solutions and reasonable strategies that can help your company minimize your risk.

# Sample Contracts and Documents

## Chapter 15

# Acceptable Use Policy

In the event that an employee uses company computer and communication systems to copy copyrighted material, access pornography, copy money, send fraudulent communications, etc. your company will be better protected from liability if you have an Acceptable Use Policy Agreement in place. While there is no single “correct” policy statement, the example document below reflects the concepts covered in several good policy contracts. As always, this is only an example - you should seek advice of counsel before implementing your own version.

The acceptable use policy defines the acceptable use of computer equipment, software, communications, and equipment as provided by your company. Everyone in the company should be expected to follow the written policy without exception. The policy should be provided in writing to all employees, and signed copies of this agreement should be kept on file.

So, what defines an Acceptable Use Policy? To provide guidance as to what to place in your policy statement, let’s define a few unauthorized uses for a computer account.

The list above defines each of the specific areas of concern a company usually encounters. The following takes these concerns and places them in an appropriate text for a policy statement. Again, you should review your policies carefully, have them reviewed by legal counsel for wording and enforceability appropriate to your geographic area.

## Acceptable Use Policy Statement for Example Company

Example Company encourages the sharing of information, comprehensive access to local and national facilities to create and disseminate information, and free expression of ideas. General access facilities and infrastructure are provided to further these purposes. There is an obligation on the part of those using these facilities and services to respect the intellectual and access rights of others--locally, nationally and internationally.

Computing resources and facilities of Example Company are the property of the company and shall be used for legitimate activity related to the performance of the duties and responsibilities of the users only, administrative, public service, or approved contract purposes. Supervisors may, at their discretion, allow personal use by the employee of these resources that does not interfere with the institution or with the employee’s ability to carry out company business. Individuals who disregard elements of this policy will be subject to appropriate disciplinary and/or legal action by Sample Company. Use of company computing facilities for personal or commercial use is not authorized. Use of company computing facilities for educational purposes must be consistent with other training educational programs. The use of company

computing facilities for higher education degree seeking or certification programs may only be done with the specific written approval of the appropriate supervisor.

Individuals and non-company organizations using the company's facilities to gain access to non-company facilities must be cognizant of and observe the acceptable use policies of the company at all times.

Failure to observe these policies will result in immediate disconnection or loss of use privileges, as well as possible disciplinary action or termination at the discretion of the offending party's supervisor or department head based on the nature and severity of the offense.

## Company Policies

1. Users will not violate copyright laws and their fair use provisions through inappropriate reproduction and/or distribution of music (MP3, etc.), movies, computer software, copyrighted text, images, etc.

2. Users shall not use company computers or network facilities to gain unauthorized access to any computer systems. Using programs intended to gain access to unauthorized systems for any reason or purpose is strictly prohibited.

3. Users shall not connect unauthorized equipment to the company's network, to include hubs, routers, printers or other equipment connected to the company's network directly or via remote attachment.

4. Users shall not make unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.

5. Users will not associate unapproved domain name sites with a company owned IP address.

6. Users will not knowingly or carelessly perform an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.

7. Users will not knowingly or carelessly run or install on any computer system or network, or give to another user, a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, and worms.

8. Users will refrain from activity that wastes or overloads computing resources. This includes printing too many copies of a document or using excessive bandwidth on the network.

9. Users will not violate terms of applicable software licensing agreements or copyright laws.

10. Users will not use company resources for commercial activity, such as creating products or services for sale.

11. Users will not use electronic mail to harass or threaten others, or to send materials that might be deemed inappropriate, derogatory, prejudicial, or offensive. This includes sending repeated, unwanted e-mail to another user.

12. Users will not use electronic mail on company-owned, or company-sponsored, or company-provided hardware or services to transmit any information, text, or images that would be deemed offensive, inappropriate, derogatory, prejudicial, or offensive.

13. Users will not initiate, propagate or perpetuate electronic chain letters.

14. Users will not send inappropriate mass mailings not directly associated with, or in the performance of, the routine course of duties or assignments. This includes multiple mailings to newsgroups, mailing lists, or individuals, e.g. "spamming," "flooding," or "bombing."

15. Users will not forge the identity of a user or machine in an electronic communication.

16. Users will not transmit or reproduce materials that are slanderous or defamatory in nature, or that otherwise violate existing laws, regulations, policies, or which are considered to generally be inappropriate in a work place.

17. Users will not display images or text that could be considered obscene, lewd, or sexually explicit or harassing in a public computer facility or location that can be in view of others.

18. Users will not attempt to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

19. Unauthorized viewing or use of another person’s computer files, programs, or data is prohibited. All users should also be aware that all programs and all files are deemed to be the property of the company, unless the individual has a written agreement signed by an appropriate representative or officer of the company. Federal or state law may require disclosure of individual computer files which are deemed public records under the state public records statute and that state and federal law may prohibit the disclosure of certain records as well.

20. Entry into a system, including the network system, by individuals not specifically authorized (by group or personally), or attempts to circumvent the protective mechanisms of any system, are prohibited. Deliberate attempts to degrade system performance or capability, or attempts to damage systems, software or intellectual property of others are prohibited.

21. The electronic mail system shall not be used for "broadcasting" of unsolicited mail or for sending chain letters, and the communication system shall not be used for sending of material that reasonably would be considered obscene, offensive, or threatening by the recipient or another viewer of the material.

22. The company reserves the right to monitor and record the usage of all facilities and equipment, and all software which is the property of the company by ownership, lease, rent, sponsorship or subsidy, if it has reason to believe that activities are taking place that are contrary to this policy or state or federal law or regulation, and as necessary to evaluate and maintain system efficiency. The company has the right to use information gained in this way in disciplinary or criminal proceedings.

23. The Federal Copyright Act nearly always protects commercial software. Use of company facilities or equipment for the purpose of copying computer software that does not contain specific permission to copy (some licenses do allow the making of one copy for backup) is prohibited. The unauthorized publishing of copyrighted material on a company server is prohibited, and users are responsible for the consequences of such unauthorized use.

24. An individual's access to computer resources may be suspended immediately upon the discovery of a violation of this policy.

This policy contains the company's complete acceptable use policy and replaces any pre-existing policy issued before *Month Day, Year*. For questions about this policy, contact *Name and Contact Information here.*

Failure to comply with any of the above policies may result in termination of your Example Company network services, disciplinary action, and/or criminal prosecution. The company reserves the right to terminate any company network connection without notice if it is determined that any of the above policies are being violated.

# Sample E-mail/Internet User Agreement

**Employee Agreement:**

I have received a copy of Example Company's Corporate Policy Guideline on e-mail/Internet acceptable use, policy #_____, dated, _____. I recognize and understand that the company's e-mail/Internet systems are to be used for conducting the company's business only. I understand that use of this equipment for private purposes is strictly prohibited.

As part of the Example organization and use of Example's gateway to the Internet and e-mail system, I understand that this e-mail/Internet corporate guideline applies to me. I have read the aforementioned document and agree to follow all policies and procedures that are set forth therein. I further agree to abide by the standards set in the document for the duration of my employment with Example Company. I am aware that violations of this corporate guideline on e-mail/Internet acceptable use may subject me to disciplinary action, up to and including discharge from employment.

I further understand that my communications on the Internet and e-mail reflect Example Company, worldwide to our competitors, consumers, customers and suppliers. Furthermore, I understand that this document can be amended at any time.

_____

Employee Signature Date

_____

Employee Printed Name

_____

Manager Signature

**You should communicate this policy in several ways, including:**

1. On-line message that appears when the user logs onto e-mail/Internet.
2. Short policy statement regarding e-mail/Internet acceptable use in the employee handbook.
3. Orientation and hiring statement notifying new employees of e-mail/Internet policies.
4. Training Sessions on computer and Internet use and e-mail policies. An employee who is told that monitoring will occur may be apprehensive about using the company's e-mail and Internet systems. Training sessions where policies are explained in detail can go a long way in allaying fears.

# Sample Privacy Statement

Example Company understands the importance of protecting the privacy of our customers and others who visit our Web site. We consider any personal information you may supply to us to be personal and confidential, and we are committed to using this information solely for the purpose of providing you with superior service and convenient access to the right products and services.

We take our commitment to safeguarding customer information seriously, which is why we have adopted the following principles:

1. Example Company makes every effort to collect, retain, and use customer information only where we believe it is useful (and as allowed by law) in administering Example Company business and to provide products, services, and other opportunities to our customers.

2. Example Company limits employee access to personally identifiable information to those with a business reason for knowing such information. Example Company stresses the importance of confidentiality and customer privacy in the education of its employees. Example Company also takes appropriate disciplinary measures to enforce employee privacy responsibilities.

3. Example Company does not disclose our customers' personal or account information to unaffiliated third parties, except for the transferring of information to reputable credit reporting agencies; or when the information is provided to help complete a customer initiated transaction; the customer requested the release of the information; or the disclosure is required or allowed by law.

4. Example Company maintains appropriate security standards and procedures regarding unauthorized access to customer information.

5. If Example Company provides personally identifiable information to a third party, we insist that the third party adhere to similar privacy principles that provide for keeping such information confidential.

# Company Acceptable Internet Use Policy

If a user violates any of the acceptable use provisions outlined in this document, his/her account will be terminated and future access will be denied. Some violations may also constitute a criminal offense and may result in legal action. Any user violating these provisions, applicable state and federal laws, is subject to loss of access privileges and any other Company disciplinary options.

1) Acceptable Use

- Must be in support of education and research consistent with company policy, and employees job description
- Must be consistent with the rules appropriate to any network being used/accessed
- Unauthorized use of copyrighted material is prohibited
- Publishing, downloading or transmitting threatening or obscene material is prohibited
- Distribution of material protected by trade secret is prohibited
- Use for commercial activities is not acceptable
- Product advertisement or political lobbying is prohibited

2) Privileges

- Access to the Internet is not a right, but a privilege
- Unacceptable usage will result in cancellation of account, and possible disciplinary proceedings

3) Netiquette

- Be polite
- Do not use vulgar or obscene language
- Use caution when revealing your address or phone number (or those of others)
- Electronic mail is not guaranteed to be private
- Do not intentionally disrupt the network or other users
- Abide by generally accepted rules of network etiquette

4) Security

- If you identify a security problem, notify a system administrator immediately
- Do not show or identify a security problem to others
- Do not reveal your account password or allow another person to use your account
- Do not use another individual's account
- Attempts to log on as another user will result in cancellation of privileges

- Any user identified as a security risk or having a history of problems with other computer systems may be denied access
- User must notify the system administrator of any change in account information
- User may be occasionally required to update registration, password and account information in order to continue Internet access
- Company has access to all mail and user access requests, and will monitor messages as necessary to assure efficient performance and appropriate use.

5) Vandalism/Harassment

- Vandalism and/or harassment will result in the cancellation of the offending user's account
- Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet or other networks. This includes, but is not limited to, creating and/or uploading computer viruses
- Harassment is defined as the persistent annoyance of another user or the interference in another user's work. This includes, but is not limited to, the sending of unwanted mail

6) Penalties

- Any user violating these provisions, applicable state and federal laws or posted company rules is subject to loss of network privileges and any other Company disciplinary options, including criminal prosecution

- All terms and conditions as stated in this document are applicable to all users of the network. This policy is intended to be illustrative of the range of acceptable and unacceptable uses of the Internet facilities and is not necessarily exhaustive.

I understand and will abide by the Company Acceptable Internet Use Policy. I further understand that any violation of this Acceptable Internet Use Policy is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

User Signature:_____ Date:_____

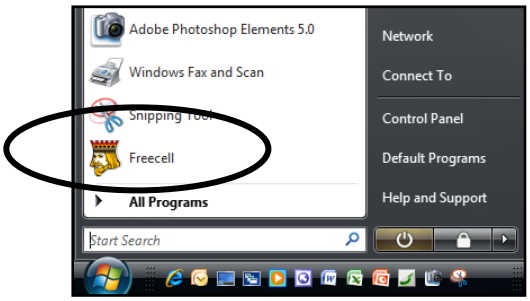
# Computer Bread Crumbs

## Chapter 16

## Computer Forensics

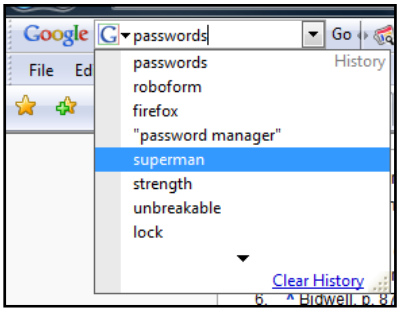
It is fairly easy to see what a person has been doing on their computer. Of course there may be serious legal issues related to the inspection of another person's computer, but for purposes of this chapter let us assume that you have the legal right to inspect the computer in question. Whether it is an employee, a child, a spouse or some other person, you can inspect their computer usage a number of ways, as follows:

1. **Recent Applications -** The Start Button in Windows displays recently used applications. Therefore if an employee has been playing games on the job, you can see this easily see the application icon displayed in the Program list. For example, the user below has recently launched the FreeCell application.

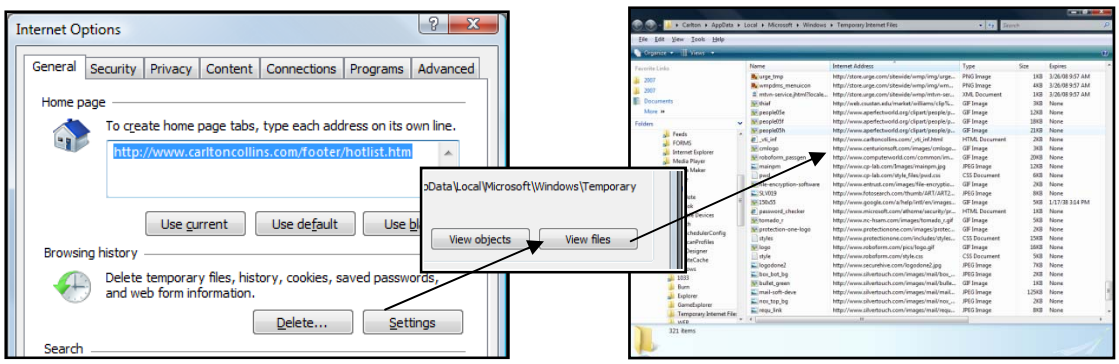



2. **Game High Scores** – If an employee denies playing games, you can check the high scores to see if the game has indeed been played. Also, a very high score might tell you that the employee has spent a great deal of time learning to play that particular game. (High scores can usually be reset to defeat this bread crumb).

3. **Search history –** Most search tools keep a log of recently searched terms. As shown below the Google toolbar displays recently search for phrases through the simple drop down arrow. (Search Histories can usually be reset to defeat this bread crumb).

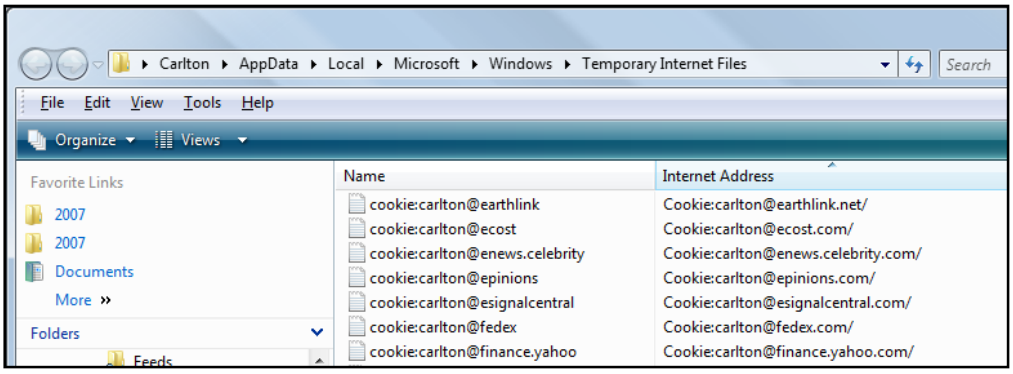



4. **Browsing History** – In most browsers, you can drill to a cache of browsing history, as show in the screen below (In Internet Explorer, choose Tools, Options. As shown below, this Settings, View Files Buttons display a list of web site objects (web pages, pictures and objects) that have been viewed.




The data in this screen is a little cryptic, but you generally can pick out the URLs that have been visited. You can also double click on any item in the list to display that web page, image or object. If a person has been visiting and inappropriate web site, you can probably see those tracks here. In addition, the browser keeps track of the date and times these web sites were last visited, providing solid proof as to how a computer was being used during business hours. (Browsing Histories can be reset to defeat this bread crumb. Further the amount of space used for capturing browsing histories can be set to zero in order to prevent this bread crumb).

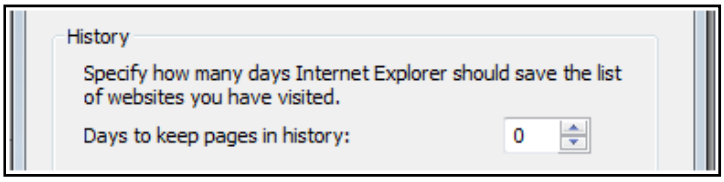
5. **Cookie History** – Many web sites deposit cookies on your computer. Cookies are harder to avoid because many web sites require cookies in order to work properly. Therefore if a user deletes or blocks cookies from their computer, then they cannot access the web site. The Cookies screen shown below shows that this user has visited the web sites for FedEx, Earthlink, eCost, epinions, Yahoo Finance, and eNews – among others. In addition, the browser keeps track of the date and times cookies were last updated, providing solid proof as to how a computer was being used during business hours.




(Cookies can be erased individually to defeat this bread crumb, but doing so is tedious. The user is not likely to delete all cookies as some of them are probably important to the accessibility of web sites.)

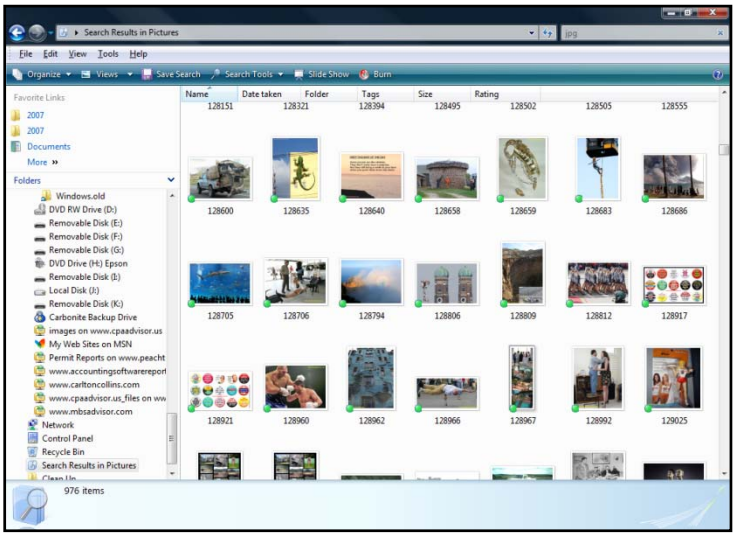
6. **Temporary Internet Files** – Most browsers also keep a history of temporary internet files, which makes it much faster for a user to browse backwards to recently displayed web sites using the back button. Temporary Internet Files are like Browsing History files,

but they are kept in a separate folder. In Internet Explorer, these files are accessed through the Tools, Options dialog box under Browsing Settings.




(Temporary Internet files can be set to "zero days" in order to defeat this bread crumb.)

7. **Search for JPGs** – If an employee or child is viewing inappropriate pictures on the Internet, they might also take the next step of saving them to their computer. You can use the built in search tools in Windows to search of JPGs or other picture formats such as BMPs or Tiffs. In the screen below the search for JPG has reveals more than 900 such pictures. From here it is easy to scan the pictures to determine if any are inappropriate.




8. **Recycle Bin** – An employee or child trying to cover their tracks might delete pictures or other files from their computer, but they might not be clever enough to remember to empty their recycle bin. When files are erased in Windows, they are not really erased until the recycle bin is emptied. Therefore a quick peek at the recycle bin might be very revealing. (This bread crumb can be defeated by emptying the recycle bin).

9. **Password Protected Files** – If an employee or child has password protected files on their computer, you may be able to open them with commonly available hacker tools. This is true particularly for Word and excel 2003 documents (and earlier). These tools are discussed in the hacking and cracking chapter.

10. **Requesting Lost Passwords** – In the event that you want to review your child's MySpace or Facebook accounts, and the child refuses to provide you with the proper password,

you could attempt to log into an account, click the forgotten password button, and an e-mail will most likely be sent to that computer enabling you to reset the password.

11. **Review Sent and Received E-Mail** – Of course it should be obvious that you could review the sent and received e-mail of an employee or child in an effort to identify inappropriate computer usage.

12. **Review Deleted E-Mail Folder** – Of course an employee or child may be clever enough to delete their inappropriate sent or received e-mail messages, therefore you might want to inspect the Delete E-mail Folder. Like the recycle bin, most deleted e-mails are not actually deleted until the Delete Folder is emptied.

13. **Review Junk E-Mail Folder** – Of course an employee or child may be smart enough to delete their sent or received e-mail, therefore you might want to scan the deleted e-mail folder. Like the recycle bin, most deleted e-mails are not actually deleted until the Delete Folder is emptied.

14. **Use E-Mail Rules to Track Usage** – A stronger measure would be to set up e-mail rules on the computer in question. For example, you could set up a rule that forwards a copy of all e-mail to your account, or just those e-mails from certain persons or those that contain certain words. Chances are good that these rules will be undetected by the user.

15. **Use E-Mail Server Settings to Track Usage** – A better way to track the users e-mails would be to set up the mail server to forward a copy of all messages, sent or received, to your e-mail address. You might also use a rule on your computer to send these messages automatically to a specified folder.

16. **Tools to help You Track Computer Usage**

    a. **Key Loggers** – You could download and install a key logger on the computer in question. This tool would capture all keystrokes typed into the computer and would later allow you to identify passwords used by the user. This is a fairly significant step, but downloading and installing a key logger is relatively easy – it takes about 3 to 5 minutes. KGB (free), ActualSpy ($60), and Family Keylogger (free) are examples of key loggers.

    b. **Print Monitor Pro (free)** – Once installed, this tool captures a screen shot of every document printed from the computer and stores those images in a database.

    c. **Give Me Do (free)** – This tool captures all visited Web pages, sent and received emails and stores them to a folder of your choice.

d. **Desktop Spy (free)** - Monitors the activity of users on a PC by automatic capturing of desktop/active application screenshots and saving them to a specified directory on the hard drive.

e. **Hardware Keylogger ($60)** – USB device plugs into a computer, and automatically captures all keystrokes entered into the keyboard. Very stealth.



f. **Internet Spy (free)** - Freeware utility that continuously monitors every Web page accessed on the computer and makes a chronological record of all visited URLs.

g. **Evidence Tracker** - EvidenceTracker.com "ET" is one of the very first entirely browser based evidence tracking applications for police and law enforcement agencies. This software is ideal for agencies that track evidence from the point of delivery by an officer until it is ordered to be destroyed. The ET system allows users to track evidence through the entire process and to print out all the necessary reports for internal or court purposes. Tracker Products Software is used in a variety of industries including law enforcement, forensic analysis, legal, museums, gaming, construction, manufacturing and hospitals just to name a few. The system customization feature allows your organization to tailor the software to meet your particular needs. All item entry screens can be modified to collect the information that is important to you. Why settle for a software package that requires expensive customization upgrades? Tracker Products software will work for you!

17. **Evidence Blaster ($23)** – Not to be outdone, Evidence Blaster is a product that deletes all evidence of pornography from your computer.

**Microsoft COFEE -** Microsoft offers a small plug-in device that investigators can use to quickly extract forensic data from computers that may have been used in crimes. The COFEE, which stands for Computer Online Forensic Evidence Extractor, is a USB "thumb drive" that was quietly distributed to a handful of law-enforcement agencies in June, 2007. The device contains 150 commands that can dramatically cut the time it takes to gather digital evidence, which is becoming more important in real-world crime, as well as cybercrime. It can decrypt passwords and analyze a computer's Internet activity, as well as data stored in the computer. This device eliminates the need to seize a computer, which typically involves disconnecting from a network, turning off the power and potentially losing data. Instead, investigators can scan for evidence on site. More than 2,000 officers in 15 countries, including Poland, the Philippines, Germany, New Zealand and the United States, are using the device, which Microsoft provides free.

# Computer Disposal

## Chapter 17

## Computer Disposal

It is estimated that 45 million computers become obsolete each year. This situation creates two problems – protecting information and disposing of your old computers. Most organizations store their old computers, which serve as backup equipment in case newer computers break down. These old computers often sit in storage well beyond their potential useful life. At some point, a decision must be made about disposal of this equipment. Continuing to store it is often not a viable option, because it eventually takes up a considerable amount of space. The least desirable option is to throw old computers in the garbage. Not only are there the potential liabilities and disposal costs imposed by state and federal environmental agencies, there is also the possibility of someone removing hard drives and recovering sensitive data. To combat these problems, you should follow a good disposal strategy.

## Computer Disposal Comments

1. **Federal Environmental Law** - The Resource Conservation and Recovery Act (RCRA) has been updated recently to include guidelines regarding the disposal of computer monitors.
2. **Sarbanes Oxley and HIPPA -** Sarbanes Oxley and HIPPA laws require that all data be properly removed before hard drives are properly disposed of.
3. **Hazardous Materials** - Computers contain hazardous materials such as mercury, cadmium (a known carcinogen), and hexavalent chromium (associated with high blood pressure, iron-poor blood, liver disease, and nerve and brain damage in animals).
4. **CRT Concerns** - Most environmental concerns are associated with monitors. Specifically, a color cathode ray tube (CRT) contains about four to five pounds of lead, which of course is considered hazardous waste according to the EPA.

5. **Computers in Landfills Outlawed -** California, Massachusetts, and Minnesota have outlawed the disposal of computer waste in landfills.
6. **Ponder This -** Suppose what might happen if groundwater becomes contaminated and a search for the source finds that your old computer (identified by a control tag or manufacturer's number) has been discarded nearby. You could be subject to potentially costly criminal and civil litigation (i.e., SARA, formerly CERCLA, litigation). This could happen even if the organization had donated the equipment to a charity or paid a company to recycle it.
7. **License Considerations -** If you donate your computer, you should evaluate software license agreements to determine if they preclude transfer of the software along with the computer.

## Computer Disposal Procedures

1. **Remove Data and Information -** Before disposing of your computers you must remove all information from the computer before giving it away, donating it, throwing it away, or shredding the computer. Simply deleting files does not prevent them from being recovered from the hard drive; sometimes, files can even be retrieved from reformatted drives, depending upon which operating system is used to reformat the hard drive. Here are your legitimate options for removing data:

    a. ***Erase Files*** *– Simply erasing files is* ***not good enough****, your data is still there and readable.*

    b. ***Reformat Hard Drive*** *– Reformatting the hard drive is* ***not good enough*** *- your data is still there and readable.*

    c. ***Hard Drive Eraser Tools*** *– To properly erase a hard drive, you must use a software program designed to clean the hard drive. Here are a few such tools:*

| | |
|---|---|
| 1. *BCWipe - Free* | 2. *DriveScrubber - Free* |
| 3. *Paragon Hard DiskManager - Free* | 4. *Eraser for Windows* |
| 5. *Darik's Boot & Nuke* | 6. *ActiveKillDisk – Free* |
| 7. *PC Inspector e-maxx* | |

    These tools work using one of the following erasure methods:

    i. *Quick Erase: Fills hard drive with 0's*
    ii. *Gutmann: 27 random-order passes using specific data combined with eight passes using random data. Due to changes in the different data encoding schemes now used by modern hard drives, Gutmann no longer recommends 35 passes. A few random passes should suffice.*

iii. *American DoD 5220-22.M: A seven-pass wipe using random characters, complements of characters, and random data streams.*
iv. *Canadian RCMP TSSIT OPS-II: 8 drive-wiping passes with a random byte in the overwrite sequence changed each time.*
v. *PRNG Stream methods: Overwrites the drive with a stream from a Pseudo Random Number Generator (PRNG)*

2. **Tagging –** In larger organizations, computer equipment that is not likely to be used again should be tagged for disposal, and disposed of in bulk each year.

3. **Remove Company IDs –** You should consider removing all company insignia and inventory control tags from computers to be disposed of. This step might hamper hackers from identifying any data to which company any recovered information belongs or might prevent liability in the event that the computer's new owner throws it in a land fill.

4. **Keep the Hard Drives** – Some companies find it easiest to simply remove the hard drives and keep them in storage forever rather than going through the trouble of removing files. They are easy to remove and small enough to keep. Also, this may act as a rudimentary backup measure.

If you do follow this procedure, it might be helpful to notate on each hard drive the size, date, and brief description of the contents of the hard drive before storing.

5. **Recycling Programs -** Many computer manufacturers and computer hardware manufactures also have their own recycling and/or trade in programs. Below is a list of some of the major manufactures and links to their recycling programs.

    a. Apple recycling program
    b. Dell recycling program
    c. Epson recycling program
    d. Gateway recycling program

e. Hewlett Packard recycling program
f. IBM / Lenovo recycling program
g. Lexmark recycling program
h. NEC recycling program

6. **Recycling Companies** - Below is a short list of some of the major recycling companies capable of recycling computers.

    a. E-Tech Recycling (http://www.etechrecycling.com/)
    b. Genesis Recycling (http://genesisrecycling.ca/)
    c. IBM PC Recycling (http://www.ibm.com/ibm/environment/products)
    d. Intercon Solutions (http://www.interconrecycling.com/)
    e. Back Thru the future, Inc. (http://www.backthruthefuture.com)
    f. Envirocycle Inc. (http://www.enviroinc.com)
    g. Total Reclaim (http://www.totalreclaim.com/)
    h. United Recycling Industries (http://www.unitedrecycling.com)
    i. National Revitalization Services (http://www.natrs.com/)
    j. Share The Technology: (http://sharetechnology.org)
    k. National Cristina Foundation: (http://www.cristina.org)
    l. Recycles.org: (http://www.recycles.org/)
    m. CompuMentor: (http://www.compumentor.org/)
    n. Reboot Canada: (http://www.reboot.on.ca)
    o. RECONNECT: (http://www.reconnectpartnership.com/)
    p. Battery Solutions (http://www.batteryrecycling.com)
    q. RBRC (http://www.rbrc.com)
    r. GNB (http://www.gnb.com)

7. **Signed Agreement –** If using a recycling or disposal company, have the sign an agreement accepting responsibility for its proper disposal. This is necessary whether it is sold, given to an employee, or donated. In the event of future litigation, this documentation supports the position that the recipient has accepted responsibility for the equipment's disposal.

8. **Maintain Records –** Ask your recycling company to provide written documentation of the proper disposal of computer equipment. If a recycling company cannot or will not provide such documentation, this could be a sign that it is not a reputable company. Finally, a written record of all disposed-of computers should track the serial number, description, method of disposal, and date of disposal. This information should be kept with all other documentation regarding computer disposal.

# Back Up Strategy

## Chapter 18

## Introduction to Backup Strategy

A computer back up is like insurance – you sincerely hope that the effort and money invested in both your insurance and backups are completely wasted. However, in the event that the worst case scenario does occur, you will be glad that you had insurance and backups. One of the most important aspects of an information security strategy is to create regular backups of computer data and applications. Given our tendency to focus on more fashionable security systems such as firewalls, intrusion detection and prevention, and anti-virus and anti-SPAM solutions, just where does data backup fit in an effective information security strategy? Quite simply, routine backup may be the most important element of all, because if these other systems and strategies fail to protect our data, backup remains our last bastion of defense.
Data backup is an essential element of any internal control system and disaster recovery plan. This chapter covers backup planning and processes, issues to be considered in implementing a backup plan, and backup media – from streaming tape, CD, DVD, external hard disks, network attached storage, to online backup.

## Data Organization

The process of backing up your data is facilitated by organizing your data properly. Some users make it a habit of saving files all over the place - in numerous separate folders including the “Desktop”, the “Program Files” folder, the “My Documents Folder”, and other folders they create. This practice can lead to file duplication, unnecessary file searching, and backup procedures that are more complicated than they need to be. You can minimize confusion and streamline backups by following these strategies:

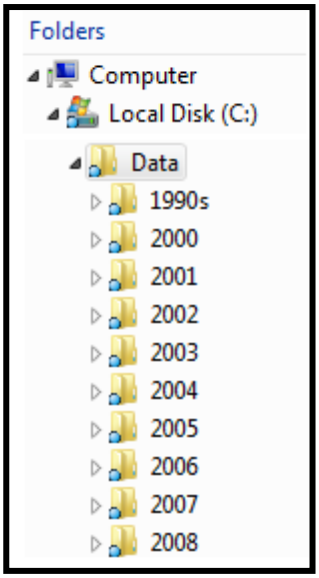
1. **One Computer Situation** - In the case on one computer system, all data should be organized under the same folder such as a “DATA” folder or the “My Documents” folder.
2. **File Server Situation** - In the case of multiple computers where a file server is present, all data should be saved to the file server, once again under the same folder such as a “DATA” folder or the “My Documents” folder.

3. **Peer to Peer Situation –** Where there are multiple computers but no file server, you should designate one of the computers to act as the file server – preferably the one that has the biggest hard drive, best performance, and is rebooted les frequently.

How your data is organized on your hard disk – the folder or directory structure – can play a significant role in the backup process. Data that is stored in a single folder or set of subfolders within a single parent folder is much easier to backup than a folder structure that stores data in numerous locations scattered across multiple folders. Microsoft applications, including Microsoft Office Small Business Accounting, routinely store all data in a folder or set of folders

within a single parent named “My Documents.” This makes it easy to create a backup plan because all data is stored in a single location. Another critical factor is how often the data changes.

You should further organize your data Under the DATA folder (or whichever folder you choose for your data) with subfolders. The particular subfolder strategy you use depends upon your situation. If you have 50 large customers, you might set up a new folder for each customer. However the approach I like best is to set up a new folder for each year, as follows:




This approach will make it easier to locate and find data, and more importantly, this approach will help you design a backup strategy that backs up your current folder more frequently than other folders.

**Identify Data to be Backed Up**

Most people seek to back up their data only, but the reality is that for each computer, you should back up your entire computer with all applications. Therefore the question as to which data should be backed up is easily answered – back up all of your computers in their entirety.

**When to Back Up**

Data that changes frequently needs to be backed up frequently. Data that changes less frequently can be backed up less often. Since operating systems and applications do not change very often, full backups can be made less frequently. Therefore you might establish a time frame for conducting your various backups as follows:

| Type of Files | Backup Frequency |
|---|---|
| 2008 Data Files (Word, Excel, etc.) | Daily |
| E-Mail Files | Daily |
| Entire Computer with all Applications | Monthly |

You should also coordinate your backup procedures with your business processes. End of month and end of year backups should coincide with the completion of write-up, adjustment, closing, and financial statement preparation processes performed by your accountant. That way your final backups will include and preserve accurate financial information.

**Backup Methods**

There are three types of backups generally used by small businesses to protect their mission critical data. The types of backup available are dependent upon the backup software used. Among the commonly used backup types available include:

- **Full Backup** – A procedure that backs up all files stored on a system, including the operating system and applications.

- **Differential Backup** – A procedure that backs up all files that have been added or changed since the last full backup.

- **Incremental Backup** – A procedure that backs up all files that have been added or changed since the last backup, regardless of whether the backup was full or incremental.

Nearly everyone understands the meaning of a full backup. The difference between a differential backup and an incremental backup requires elaboration. A differential backup is a cumulative backup. It contains all files that have been added or changed since the last full backup. An incremental backup is not cumulative. Each incremental backup only contains the files that have been added or changed since the last *incremental backup*.

Let's examine two examples to understand the difference between an incremental backup and a differential backup. ABC Company produces a full backup at the close of business each Friday.

An incremental backup is produced at the close of each workday, Monday through Thursday. ABC suffers a catastrophic failure of its primary server on Thursday. In order to fully recover all of their data, ABC must restore the last full backup and *each* of the incremental backups performed since the last full backup.

Alternatively, ABC produces a full backup each Friday and performs a differential backup each day. To recover all of their data in this circumstance, ABC must restore the last full backup and the last differential backup only. That's because a differential backup contains a cumulative backup of every file added or changed since the last full backup.

The difference between an incremental backup and a differential backup also has implications for restoring single or multiple corrupted files. A differential backup contains all files that have been added or changed since the last full backup. In order to restore a file that has become corrupted in use, just restore the file from the latest differential backup. If incremental backups were used, each backup would have to be examined in order to determine the latest version of the file in question, because the latest version of a file could be on any one of the incremental backups.

> ***Conclusion*** *– You should probably never use the incremental back up option, as it does not save much back up time and a restoration would be very complicated. The full backup or differential back up options make the most sense.*

**Selecting the Right Media**

Your back up media options are as follows:

1. Streaming Tape Cartridge
2. CDs
3. DVDs
4. USB Thumb Drive
5. SD Cards
6. External Hard Drives
7. Server Based Storage
8. Network Attached Storage
9. Online backup

Note that 1.44MB diskettes are not included in the list. The size of today's databases and the limited capacity of diskettes render them less suitable for use as backup media. These options are discussed below:


1. **Streaming Tape Cartridge -** Many large businesses use streaming tape as a backup media. These tape solutions are expensive to acquire, install and operate. You will

need to purchase a tape recording device as well such as the Dell PowerVault backup device. This option delivers is designed to archive mission-critical data in an enterprise environment. Shown below are examples of Dell's PowerVault options:


These units start at $165 and ramp up to capture 102 Terabytes.

2. **CDs** - The most common permanent backup media in use today by small businesses is writable CDs. Each CD can hold from 650MB to nearly 800MB of data. There are two types of writable CDs – CD-R and CD-RW. CD-R can be written only once. CD-RW can be written many times. In other words, data can be written to a CD-RW, erased, and then re-written multiple times. The more times a CD-RW disk is written, the less reliable it becomes for permanent backup storage. Most technicians recommend CD-R as a superior backup media. CD-R disks are inexpensive and very reliable when good quality media are used in the backup process.

   The problem with using CDs is they are very slow, but might represent a good media for backing up the current data folder.

3. **DVDs** - DVD technology and reliability are similar to CDs, but each DVD can hold 4.7GB of data on a single layer disk and nearly double that on a double layer disk. If you have large amounts of data to backup, then DVDs may be a better solution.

4. **USB Thumb Drives –** Today's thumb drives are large, fast and inexpensive. They are larger than CDs, far faster than CDs, and they are more easily reused.

5. **SD Cards** – SD cards and similar media work well, but they are more costly than thumb drives. Further, every computer, including laptops has USB ports, but not necessarily an SD Card port. Therefore USB thumb drives are considered to be the better solution compared to SD cards.


6. **External Hard Drives -** External hard disks are becoming increasingly popular for primary storage and for data backup. Units are currently priced from $49 and accommodate up to 4 terabytes of data. Examples follow:

| Device Image | USB External Hard Drive |
|---|---|
|  | Buffalo DriveStation Quattro TurboUSB HD- QS4.0TSU2/R5 - Hard drive array - 4 TB - 4 bays (SATA-150 ) - 4 x HD 1 TB - Hi-Speed USB, Serial ATA-150 (external)… $1,950 |
|  | G-Tech G-RAID mini - Hard drive array - 500 GB - 2 bays ( SATA-300 ) - 2 x HD 250 GB - FireWire 800, Hi-Speed USB, FireWire 400 (external)<br>$980 |
|  | Iomega UltraMax Pro Desktop Hard drive array - 1.5 TB - 2 bays - 2 x HD 750 GB - Hi-Speed USB, Serial ATA-300 (external)<br>$510 |
|  | Iomega UltraMax Pro Desktop Hard Drive - hard drive array<br>Hard drive array - 1.5 TB - 2 bays - 2 x HD 750 GB - Hi-Speed USB, Serial ATA-300 (external)<br>$375 |
|  | LaCie d2 Quadra Hard Disk - 500 GB - FireWire / FireWire 800 / Hard drive - 500 GB - external - FireWire / FireWire 800 / Hi-Speed USB / eSATA-300 - 7200 rpm - buffer: 16 MB<br>$165 |

These devices support the higher transfer rates of USB 2.0. These units are also true plug-n-play if Windows XP or Windows Vista is installed (there are no drivers to install – just plug it in and go). The external hard disk will automatically appear in My Computer.

7. **Network Attached Storage (NAS)** - Network Attached Storage (NAS) can be used for backup in the same way as server-based storage. Up until recently, NAS was relatively expensive for small businesses. In the past year, several vendors have modified their external hard drive products to include an Ethernet port for direct connection to a local area network. The storage is accessible as a mapped drive from any workstation desktop on your network, very similar to the way a user would attach to a network server. Examples follow:

| Device Image | USB External Hard Drive |
|---|---|
|  | IBM TotalStorage DS4800 Model 82 - hard drive array.<br>$39,700 |
|  | Intel® Entry Storage System SS4000-E. 2 TB. The SS4000-E can connect to a Gigabit Ethernet network and support up to four Serial Advanced Technology Attachment (SATA) hard disks.<br>$418 |
|  | Unibrain FireNAS™ 2U, Network Attached Storage server. Hot swap drives, and RAID protection. 12.0 TB (12,000 GB) of storage managed by a Windows® Storage Server 2003 R2. Easy installation with plug' n play connectivity.<br>$10,000 |
|  | FireDisk800-s: 500 GB hard drive.<br>$270 |

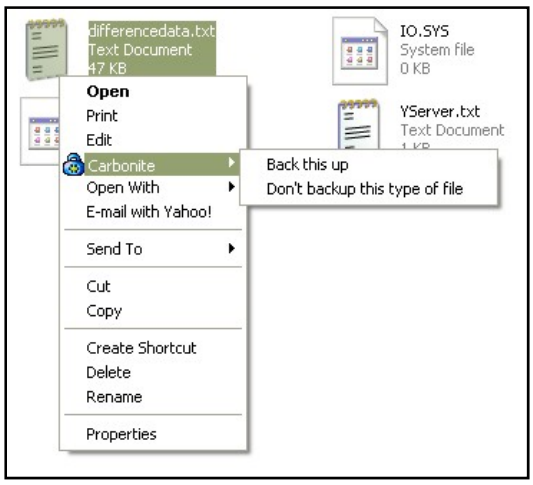
8. **Online Backup** - The latest innovation in backup media is network-based online backup. Online backup is similar in operation to a file server or NAS, but the file transfer speed is limited to the speed of your Internet connection. A typical DSL connection will have about 1/100 of the throughput of a LAN. That means that backup times will be considerably longer using online backup than backing up to a file server or NAS. Because of the slow transfer speeds, online backup is not well suited for full system backups, but is an excellent choice for financial data and documents. The chief advantages of online backup are:

    a. The backup is stored offsite
    b. The storage location is professionally managed and backed up
    c. The process is convenient because users do not have to deal with handling, storing, or administering backup media

Prices range from as little as $10 per month for 4GB of managed backup storage space. Plans typically include a backup application to schedule periodic backups from your desktop.

As an example, consider Carbonite:

For just $50 per year, Carbonite will back up all of your data. Just click on the files or folders you want to back up, and Carbonite will work in the background to keep your data in sync on a real time basis. However, I tried Carbonite with a cable connection to the Internet, and after 46 days, Carbonite still had no backed up my entire 53 GBs of data. Therefore I can conclude that Carbonite is great for backing up your current data folder, but not your entire computer system. Following is an example screen that shows how Carbonite works:



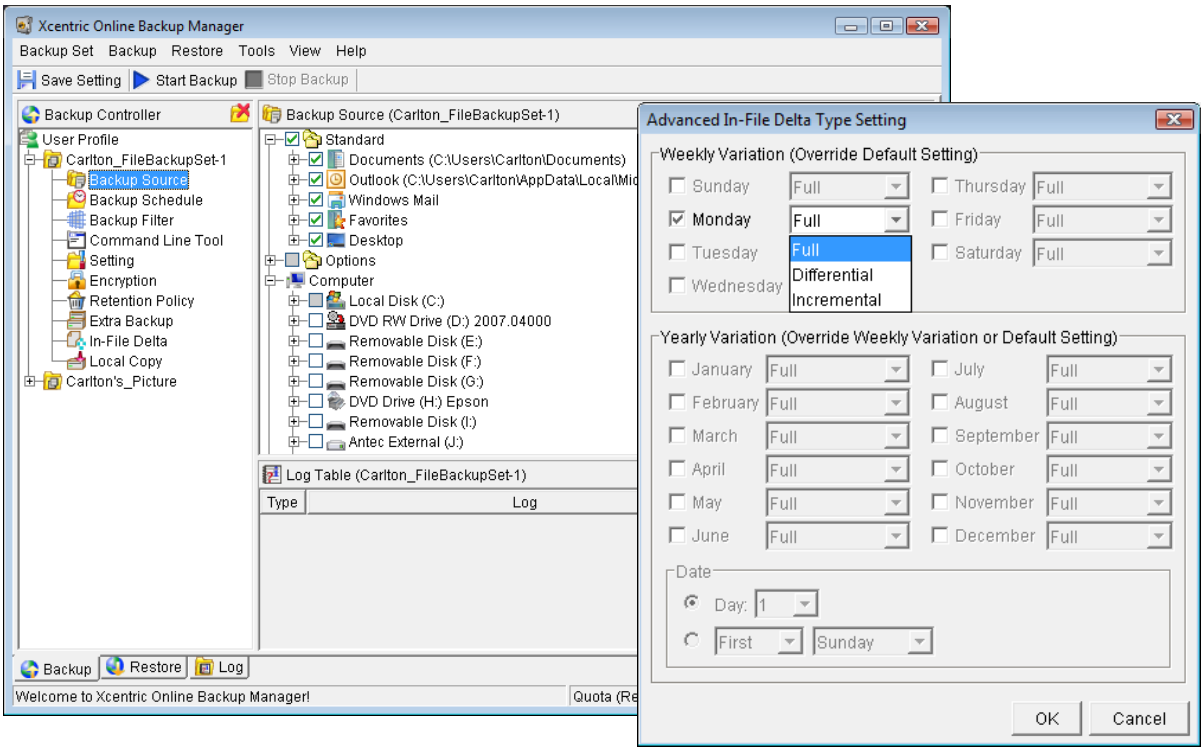

**Advantages of Each Backup Media Types**

| | Tape | CD/DVD | USB Thumb | External Disk | NAS | Online |
|---|---|---|---|---|---|---|
| Suitability for Backing Up: | | | | | | |
| Data Only | √ | √ | √ | √ | √ | √ |
| Full System | √ | | | √ | √ | |
| Backup Speed | | | √ | √ | √ | |
| Restoration Speed: | | | | | | |
| Full Restore | | √ | | √ | √ | |
| Limited or Single File | | √ | √ | √ | √ | √ |
| Portability | √ | √ | √ | | | √ |
| Suitability for Archiving | √ | √ | | | | |

## Xcentric Online Line Backup

In 2008 I tested numerous backup solutions including Carbonite, QuickBooks Online Backup, eBackups, and Xcentric. My objective was to find an inexpensive online backup system that I was happy with for my own use, and the recommend to attendees of the security course. The solution that I have been most pleased with is Xcentric Online Backup™. Here's why:

1. Completely automates the backup process.
2. Up to 2-terabytes per day
3. About $2.50 per gigabyte per month (Free 30-day trial available)
4. 128-bit encryption
5. No tapes, no hardware
6. Eliminates risk of tapes being corrupted, misplaced, damaged, or stolen.
7. Uses state of the art backup, security, and datacenter technologies.
8. Backups are fully off-site.
9. Open-file backup - if needed, you can restore data immediately– even a single file.
10. No equipment to buy
11. Simple 15-minute setup
12. Daily e-mail reporting - reports are emailed to you each day to acknowledge the success of your backups. This report also shows data backup size, remaining quota, retention copies, upload volumes, and other key information.
13. Web-based management
14. Up to 8:1 compression



Xcentric Online Backup™ security strategy includes:

| Online Backup Plans | | Paid Yearly (discounted) | Paid Monthly |
|---|---|---|---|
| Small Firms | 1 GB | $ 217 | $ 19 |
| | 3 GB | 550 | 49 |
| | 10 GB | 790 | 69 |
| | 20 GB | 1,120 | 99 |
| | 40 GB | 1,650 | 150 |
| Medium/Large Firms | 50 GB | 1,930 | 175 |
| | 100 GB | 3,250 | 299 |
| | 200 GB | 5,800 | 550 |
| | 1 TB | *Call for estimate* | |
| | 2 TB | *Call for estimate* | |
| **500 MB Trial** | | | **Free for 30 days** |

Xcentric Online Backup™ provides an average **18% savings** over the cost of traditional hardware based tape backup solutions.

**ROI | 100GB Backup**

**Traditional Tape Backup Solution**

| | Each | Yr-1 | Yr-2 | Yr-3 |
|---|---|---|---|---|
| Tape drive | $ 3,500 | $ 3,500 | $ 200 | $ 200 |
| Backup software | 750 | 750 | 250 | 250 |
| IT staffing costs (1hr/wk) | 35 | 1,750 | 1,750 | 1,750 |
| Tape media (100GB) | 70 | 2,520 | 840 | 840 |
| | **Total** | **$ 8,520** | **$ 3,040** | **$ 3,040** |
| | | | **3-Yr Cost:** | **$ 14,600** |
| | | | **Cost/month** | **$ 406** |

**Xcentric Online Backup™ Solution**

| | Each | Yr-1 | Yr-2 | Yr-3 |
|---|---|---|---|---|
| Tape drive | | 0 | 0 | 0 |
| Backup software | | 0 | 0 | 0 |
| IT staffing costs (1hr/mo) | $35/hr | $420 | $420 | $420 |
| Tape media (100GB) | | 0 | 0 | 0 |
| Xcentric Online Backup™ Services | | 3,588 | 3,588 | 3,588 |
| | **Total** | **$ 4,008** | **$ 4,008** | **$ 4,008** |
| | | | **3-Yr Cost:** | **$ 12,024** |
| | | | **Cost/month** | **$ 334** |

## Xcentric Contact Info:

Xcentric (Jason Hand), 3015 Windward Plaza, Suite 500, Alpharetta, GA 30005 - 678 297 0066 ext. 514

**Backup Rotation Scheme**

If you constantly back up your data by overwriting your previous backups, you are vulnerable in the event that your computer crashes during the backup process. You will be left with nothing. For this reason, a Backup rotation scheme must be chosen to facilitate efficient and effective backup of your mission critical data. There are several acceptable rotation schemes from which to choose. Among them are Grandfather-Father-Son (GFS) and Tower of Hanoi.2

Grandfather-Father-Son is the most widely used and easiest to understand media rotation scheme. An incremental or differential backup is made each day with a full backup made at the end of each week and the end of each month. A three week version history is preferred by information security professionals. That means that daily backups are not overwritten for three weeks.

Let's examine a practical example. ABC Company is open for business five days per week, Monday through Friday. ABC uses streaming tape with GFS and a three week version history. It requires 12 (4 days x 3 weeks) daily tapes, up to 5 weekly tapes, 12 monthly tapes, and one annual tape for a total of 30 tapes. The daily tapes are labeled D-1 trough D-12, the weekly tapes are labeled W-1 through W-5, and the monthly tapes are labeled M-1 through M-12.

The tape rotation scheme for ABC Company is illustrated in Figure 1. Notice that Tape D-1 is not reused until the first day of the fourth week in the rotation, in this case May 22nd. Tape W-1 is not reused until the following month, in this case on June 2nd.

**May - June 2006**

| Mon | Tue | Wed | Thu | Fri |
|---|---|---|---|---|
| 1 Tape D-1 | 2 Tape D-2 | 3 Tape D-3 | 4 Tape D-4 | 5 Tape W-1 |
| 8 Tape D-5 | 9 Tape D-6 | 10 Tape D-7 | 11 Tape D-8 | 12 Tape W-2 |
| 15 Tape D-9 | 16 Tape D-10 | 17 Tape D-11 | 18 Tape D-12 | 19 Tape W-3 |
| 22 Tape D-1 | 23 Tape D-2 | 24 Tape D-3 | 25 Tape D-4 | 26 Tape W-4 |
| 29 Tape D-5 | 30 Tape D-6 | 31 Tape M-1 | 1 Tape D-8 | 2 Tape W-1 |

**Monthly Grandfather-Father-Son Tape Rotation Scheme**

The monthly tapes, such as Tape M-1 used on May 31st, are taken out of the rotation and are never reused until the following year. As can be seen from this example, a three week version history means that three weeks of daily backups are produced before any tapes are overwritten.

If the Grandfather-Father-Son rotation scheme is used, here are some simple rules to make sure that your mission critical data is fully protected.

1. The daily backups should not be overwritten for a period of at least three weeks.

2. The weekly full backups should not be overwritten for at least one month.

3. The monthly full backups should be maintained and not overwritten for at least one year.

4. The annual full backup should be maintained for at least seven years, or as mandated by local regulatory requirements. Annual backups should be catalogued and maintained off site in a data vault or a fire and waterproof safe-deposit box. Duplicate copies should be maintained at different off site locations.

**Backup Archive**

Regardless of your back up methods used, you should end the year with a complete snap shot of all computers as of the end of each month or each quarter. This archive should be maintained off site. If you are using tapes, then you should be able to produce 12 tapes, each representing all computers as of the end of each month or each quarter. If you are using CDs or DVDs, then you should be able to produce 12 sets of CDs or DVDs representing computer systems as of the end of each month or each quarter. If you are using hard drives, then you should have 12 folders representing snapshots of each computer every month or for every quarter. Here is an example of what the final product should look like.

**Other Backup Considerations**

Redundant backups can be a useful technique. In other words, data could be backed up daily to a separate hard disk, file server, or NAS, as well as to permanent storage, such as CD-R or DVD. Having the same backup data stored in multiple locations provides an additional level of safety through redundancy. The greatest advantage of this technique is realized when it becomes necessary to recover a single corrupted file. Daily data backups stored on high-speed media with ready accessibility provides users with the ability to restore important files on-the-fly, without the hassle of finding and loading the latest backup media. This is especially useful in situations where backup media are taken offsite for storage. Daily backups to hard disk, a file server, or NAS should not be used alone. Make sure to backup to permanent media and store the backups offsite for maximum protection.

Offsite storage of backup media provides the greatest protection against unanticipated disasters. If your office is flooded or burns, any backup media stored in your office is likely to be destroyed or rendered unusable. Storing backups in the same location as live data does not provide sufficient protection from data loss when disaster strikes. Backup media should be stored offsite. Small businesses typically store backups at the home of the owner or a trusted employee. A better practice would be to store your backup media in a fire and waterproof safe-deposit box at your local bank.

Every business should develop a data retention policy as part of its backup plan. Governmental entities and taxing authorities regulate the retention of certain types of data. The Internal Revenue Service requires that financial and tax records be maintained for seven years. Employee payroll, benefits, and HR records should be maintained from three to seven years. Other federal agencies and some states require longer data retention periods. Your data backup plan should accommodate the regulatory framework imposed in your business location. At a minimum, long-term archive media should be generated for month-end, quarter-end, and year-end financial records. At least two copies of each archive media should be maintained, and the copies should be stored in different physical locations. Natural disaster, mishandling of media, storage in inappropriate environmental conditions, or misplacement of a single copy of critical data archives can put a company at risk.

The data backup process is fraught with potential problems that could render your backups unusable or incomplete. Media could be damaged, backup equipment may not be properly maintained, or a defined backup routine may not include a newly installed hard disk. Whatever the reason, backup is not successful unless you can get your data back! 3 The SANS Institute reports that one of the worst security mistakes made by IT professionals is their failure to maintain *and test* data backups.4 Test the integrity of your backup process by doing trial restores on a regular basis. Only then can you be confident that your backups will function in the event of hardware failure, data corruption, or natural disaster.


# Computer Viruses

## Chapter 19

## Computer Viruses

In 1986, there was only one known computer virus. By 1989 there were six and in 1990 there were 80 confirmed computer viruses. In a press release issued in June of 1999, Adam Harriss and Catherine Huneke of Computer Economics, Inc., a research firm in Carlsbad, California, stated, “The economic impact of virus and worm attacks on information systems has increased significantly this year, with businesses losing a total of $7.6 billion in the first two quarters of 1999 as a result of disabled computers.” Other surveys suggest that throughout the world, more than 60% of all companies are hit by at least one virus each year; that number is greater than 70% in the United States. Today, between 10 to 15 new viruses appear every day costing an estimated 55 billion dollars in damages (according to anti-virus company Trend Micro Incorporated). Some estimates are far higher.

Viruses come in many forms and with many different problems attached to each kind. Some viruses are designed to mess up your entire computer and destroy all data; others are made just to show you unwanted advertisements every once in awhile. Either way, they shouldn't be on your computer and can be removed by you manually or by virus removal software. The most common types of computer viruses and what they can do to you or your computer are as follows:

1. **The Worm Virus** - This type of virus can duplicate itself and it will use the email addresses from your address book, and send itself to those people. This means your friends and family computers could even become infected with this virus.

2. **The Trojan Virus** - This is a sneaky virus which disguises itself as a program that provides a legitimate function. But really it is a virus that will damage your computer or steal personal information like passwords.

3. **The Backdoor Trojan Virus** - If your computer was infected with it, someone could take control of your computer through your network or the internet.

4. **File Virus** - File viruses can attach to real software, so that whenever you use the software, it will load into your memory and infect other files that are associated with that program. That means that the most important documents and data could be destroyed by one simple click.

5. **Adware and Spyware** - Adware is basically just advertisements that are saved on your computer, and show themselves sometimes in a random pop-up or when you type in a web address that is incorrect. Spyware is actually the worst of the two because spyware can log your every keystroke, record every website you go to, and report your statistics back to an individual or company.

## Important Virus Tips

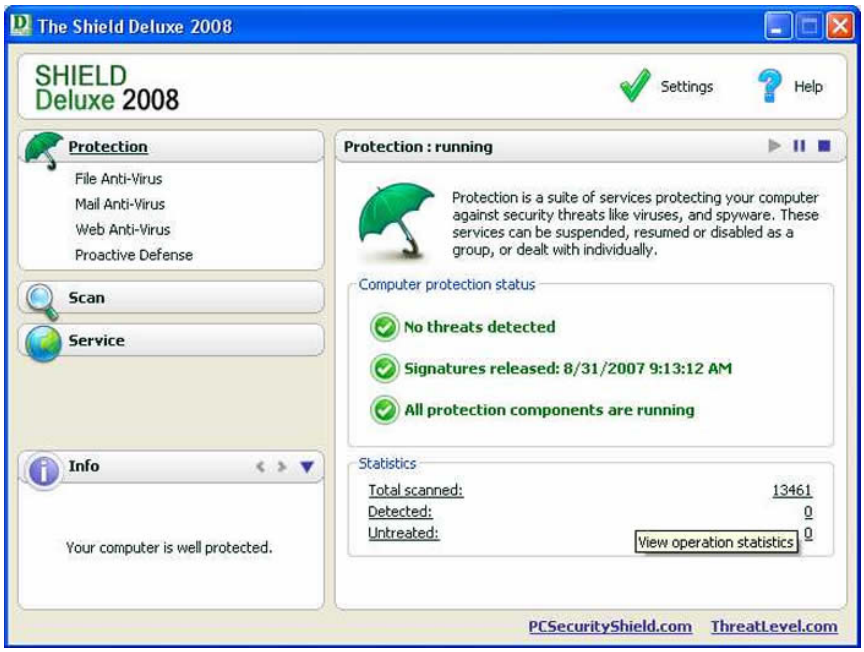
To recover from a computer freezing virus, you should take these steps:

1. Make a backup copy of your hard drives data every week.
2. Backup your BIOS every time you change it or a part on your computer.
3. Run virus protection software.

Viruses are a fact of life that we all must contend with. Luckily, virus protection technology has never been better, and there are dozens of such products to choose from. Presented below is a listing of ten of the best antivirus products on the market, followed by a brief description of 3 of the most recommended solutions.

| | | |
|---|---|---|
| 1. | BitDefender | 24.95 |
| 2. | CA | 39.99 |
| 4. | The Shield Deluxe | 29.99 |
| 5. | Panda | 39.95 |
| 6. | TrendMicro | 39.95 |
| 7. | McAfee | 39.99 |
| 8. | NOD 32 | 39.99 |
| 9. | Norton | 39.99 |
| 10. | Kaspersky | 59.95 |

**The Shield Deluxe 2008** is a rather simple to use anti-virus software and anti-spyware program. It is relatively painless to download, install and use.



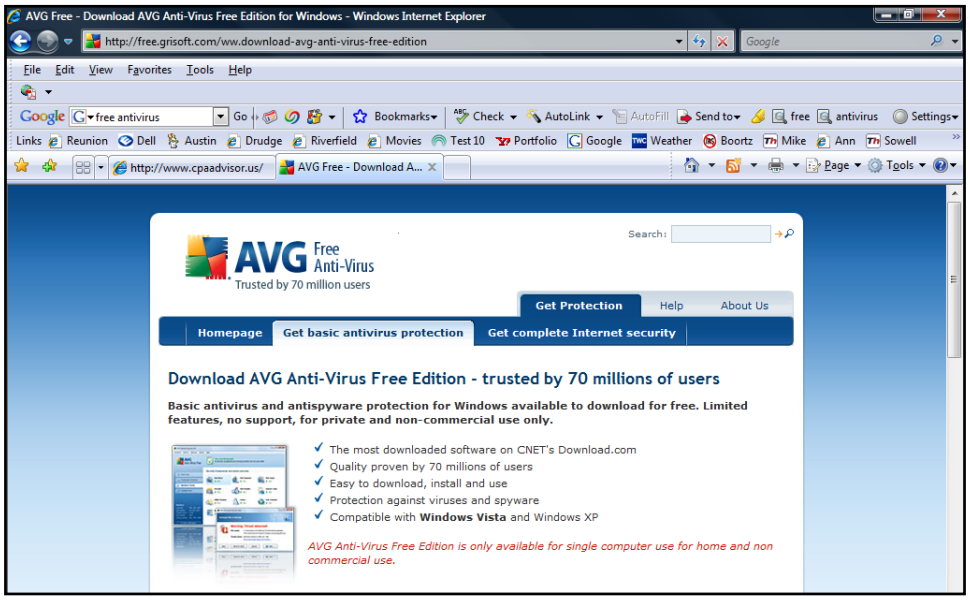
**The Shield Deluxe** anti-virus software comes with an installation utility that detects remnants of previously installed anti-virus software, weeding them out before the download begins. The Shield Deluxe 2008 has automatic updates and weekly virus scans are all pre-scheduled. It is Vista Compatible and you can use this **Special 20% Off Coupon - PCSS20** (Apply Coupon in shopping cart).

**CA anti-virus software** has such a clean interface with what seems to be a very high "install and forget rating". There is no overload of information and choices on the interface which is good. CA Anti-virus's main software component runs at less than 13mb RAM which is pretty light and my overall system scan was pretty fast.

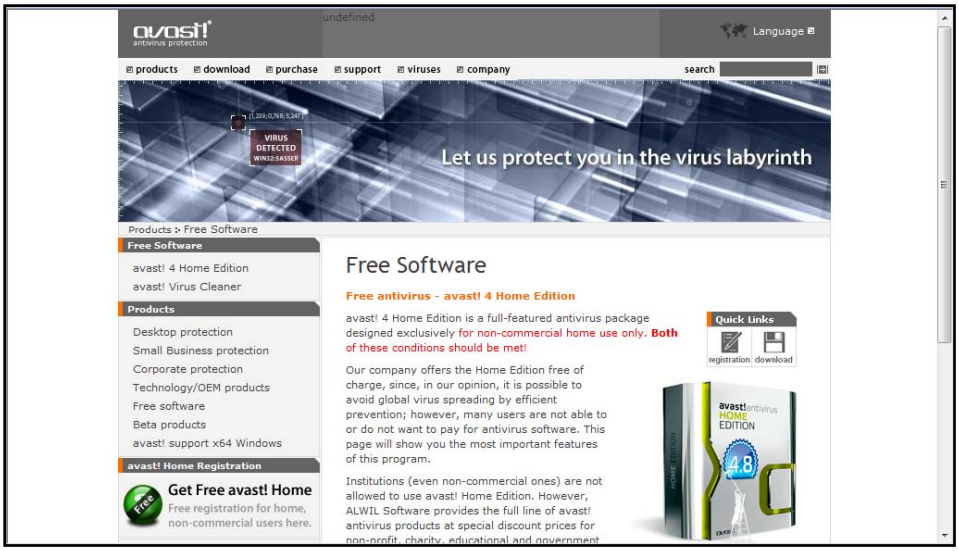

**Trend Micro's Anti-virus plus Anti-spyware** provides tools to battle malicious spyware, amongst things like trojans, hackers, worms, and adware. The anti-virus software component is an easy to use product but after that, the rest of their software can be somewhat confusing for a computer user with less knowledge.

# Free Anti-Virus Programs

AVG - is one of the most often recommend freeware anti-virus packages. While Grisoft offers a paid version, there is a freeware version of the virus protection on the website. It only offers virus protection (no anti-spam, anti-spyware or firewall) but is said to be very effective at that task. Highly recommended, but you'll need to add spyware protection separately. There is a free AVG Anti-Spyware add-on, but it doesn't do automatic updates, so unless you are diligent to keep it updated, I'd recommend against it.




**Avast!** - another freebie anti-virus program with basic features, and ease of use. It is updated regularly, also highly recommended. But again, it offers only anti-virus protection, unless you pay for the Avast Professional version.



**Avira Anti-Vir** - Free Antivirus program, which offers: Extensive Malware Recognition of viruses, Trojans, backdoor programs, worms, etc. Automatic incremental updates of antivirus signatures, engine and entire software. Permanent virus protection, with Virus Guard real time monitoring. Install and configuration in just a couple of steps. Virus protection against known and unknown threats, using an advanced heuristic system. Scheduler where you can set the scanner to make automatic virus scans or updates on your system. Forum and phone support, Knowledge Base with virus descriptions available on web site. Vista Support. Rootkit Detection and Removal. Version 8 adds an enhanced interface, a modularized AV-search engine for improved scan performance, and an failsafe security system.

# Phishing

# Chapter 20

## Phishing

Phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. eBay, PayPal and online banks are common targets. Phishing is typically carried out by email or instant messaging, and often directs users to enter details at a website, although phone contact has also been used. Phishing is an example of social engineering techniques used to fool users.

In 2007 phishing attacks escalated as 3.6 million adults lost $3.2 billion in the 12 months ending in August 2007 – up from 1.2 million computer users and an estimated $2 billion between May 2004 and May 2005.

The first recorded use of the term "phishing" was made in 1996 and alludes to the use of increasingly sophisticated baits used in the hope of a "catch" of financial information and passwords.

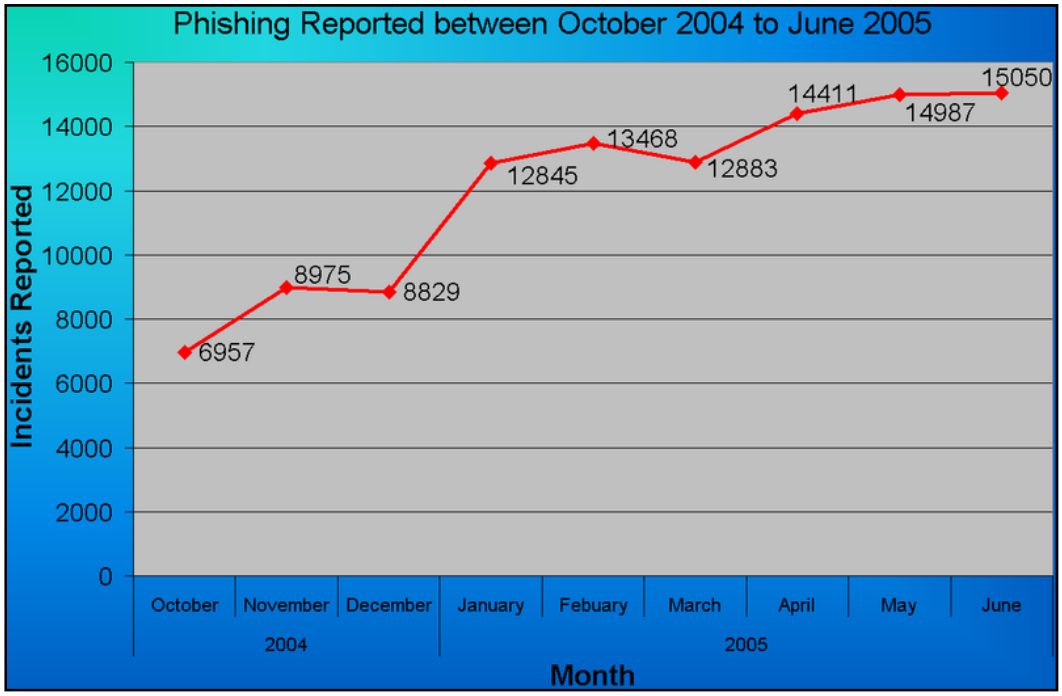
A phishing technique was described in detail as early as 1987, in a paper and presentation delivered to the International HP Users Group, Interex in which phishing on AOL was closely associated with the warez community that exchanged pirated software. Those who would later phish on AOL during the 1990s originally used fake, algorithmically generated credit card numbers to create accounts on AOL, which could last weeks or possibly months. After AOL brought in measures in late 1995 to prevent this, early AOL crackers resorted to phishing for legitimate accounts.

## Transition To Financial Institutions

The capture of AOL account information may have led phishers to misuse credit card information, and to the realization that attacks against online payment systems were feasible. The first known direct attempt against a payment system affected E-gold in June 2001, which was followed up by a "post-911 id check" shortly after the September 11 attacks on the World Trade Center. Both were viewed at the time as failures, but can now be seen as early experiments towards more fruitful attacks against mainstream banks. By 2004, phishing was recognized as a fully industrialized part of the economy of crime: specializations emerged on a global scale that provided components for cash, which were assembled into finished attacks.

## Recent Phishing Attempts

A chart showing the increase in phishing reports from October 2004 to June 2005. More recent phishing attempts have targeted the customers of banks and online payment services. E-mails, supposedly from the Internal Revenue Service, have also been used to glean sensitive data from U.S. taxpayers. Targeted versions of phishing have been termed "spear phishing".




Social networking sites are also a target of phishing, since the personal details in such sites can be used in identity theft; in late 2006 a computer worm took over pages on MySpace and altered links to direct surfers to websites designed to steal login details. Experiments show a success rate of over 70% for phishing attacks on social networks.

Almost half of phishing thefts in 2006 were committed by groups operating through the Russian Business Network based in St. Petersburg.

## Phishing Techniques

1. **Link manipulation** - Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains are common tricks used by phishers. Another common trick is to make the anchor text for a link appear to be valid, when the link actually goes to the phishers' site.

   An old method of spoofing used links containing the '@' symbol, originally intended as a way to include a username and password. For example, the link http://www.google.com@members.tripod.com/ might deceive a casual observer into believing that it will open a page on www.google.com, whereas it actually directs the

browser to a page on members.tripod.com, using a username of www.google.com: the page opens normally, regardless of the username supplied. Such URLs were disabled in Internet Explorer, while Mozilla and Opera present a warning message and give the option of continuing to the site or cancelling.

A further problem with URLs has been found in the handling of Internationalized domain names (IDN) in web browsers, that might allow visually identical web addresses to lead to different, possibly malicious, websites. Despite the publicity surrounding the flaw, known as IDN spoofing or a homograph attack, no known phishing attacks have yet taken advantage of it.

2. **Filter Evasion** - Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing emails.

3. **Website Forgery** - Once the victim visits the website the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL.

   An attacker can even use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, although it is very difficult to spot without specialist knowledge. Just such a flaw was used in 2006 against PayPal.

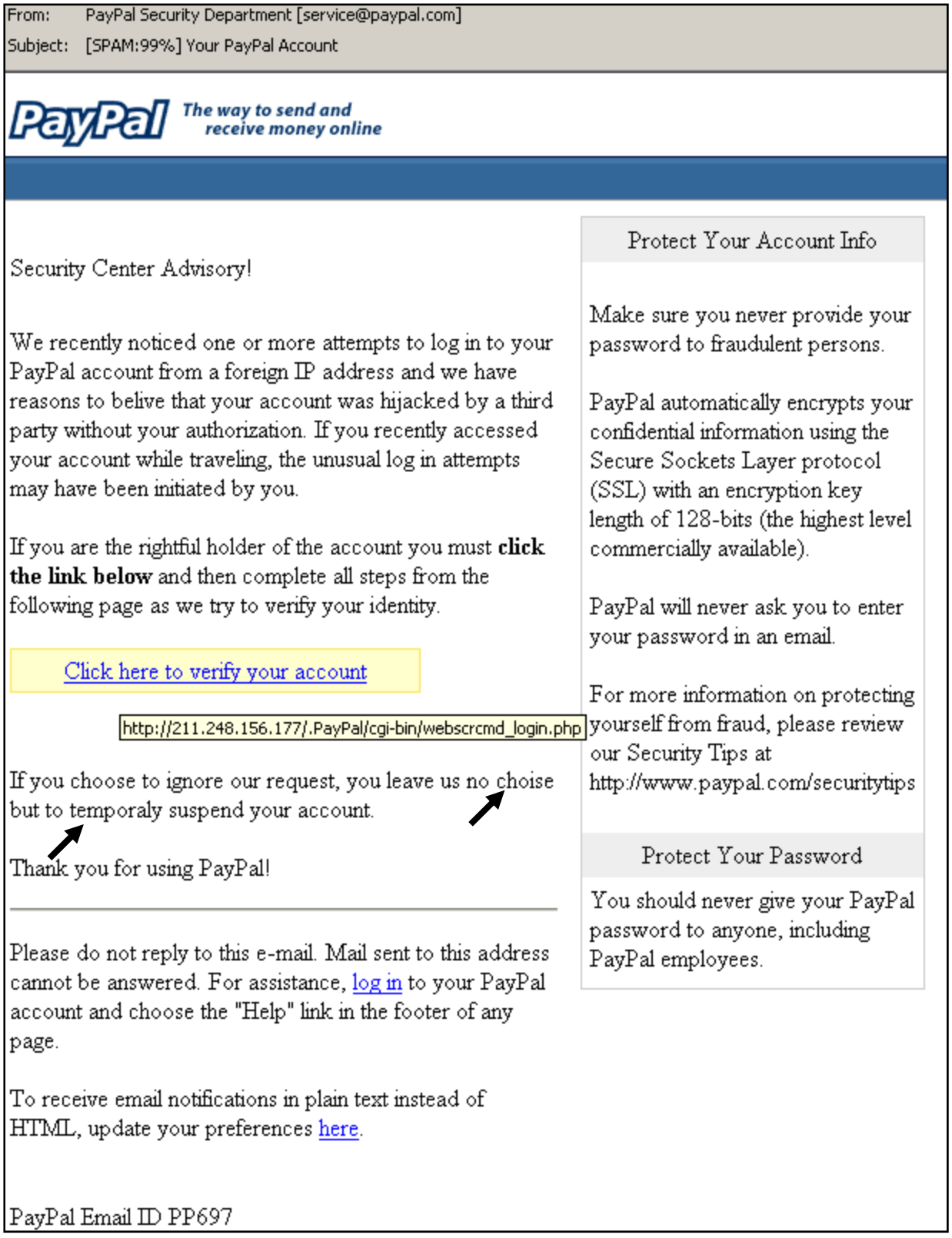
   A Universal Man-in-the-middle Phishing Kit, discovered by RSA Security, provides a simple-to-use interface that allows a phisher to convincingly reproduce websites and capture log-in details entered at the fake site.

   To avoid anti-phishing techniques that scan websites for phishing-related text, phishers have begun to use Flash-based websites. These look much like the real website, but hide the text in a multimedia object.

4. **Phone Phishing -** Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

5. **Paypal Phishing Example** – As an example, the phishing email shown below targeted PayPal users. Spelling mistakes in the email and the presence of an IP address in the link were both clues that this is a phishing attempt. Another giveaway is the lack of a personal greeting, although the presence of personal details would not be a guarantee of legitimacy. Other signs that the message is a fraud are misspellings of simple words

and the threat of consequences such as account suspension if the recipient fails to comply with the message's requests.



From: PayPal Security Department [service@paypal.com]
Subject: [SPAM:99%] Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

http://211.248.156.177/.PayPal/cgi-bin/webscrcmd_login.php

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal!

---

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

In a June 2004 experiment with spear phishing, 80% of 500 West Point cadets who were sent a fake email were tricked into revealing personal information.

## Anti-phishing Techniques

There are several different techniques to combat phishing, including legislation and technology created specifically to protect against phishing, as follows:

1. **Social Responses** - One strategy for combating phishing is to train people to recognize and to deal with phishing attempts.

2. **Check Legitimacy** - People can take steps to avoid phishing attempts by slightly modifying their browsing habits. When contacted about an account needing to be "verified" (or any other topic used by phishers), it is a sensible precaution to contact the company from which the email apparently originates to check that the email is legitimate.

3. **Look For Specifics -** Nearly all legitimate email messages from companies to their customers contain an item of information that is not readily available to phishers. Some companies, for example PayPal, always address their customers by their username in emails, so if an email addresses the recipient in a generic fashion ("Dear PayPal customer") it is likely to be an attempt at phishing. Emails from banks and credit card companies often include partial account numbers.

4. **Technical Responses -** Anti-phishing measures have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures. The following are some of the main approaches to the problem.

    a. **Helping To Identify Legitimate Sites** - Since phishing is based on impersonation, preventing it depends on some reliable way to determine a website's real identity. For example, some anti-phishing toolbars display the domain name for the visited website. The petname extension for Firefox lets users type in their own labels for websites, so they can later recognize when they have returned to the site. If the site is suspect, then the software may either warn the user or block the site outright.

    b. **Browsers Alerting Users To Fraudulent Websites** - Another popular approach to fighting phishing is to maintain a list of known phishing sites and to check websites against the list. Microsoft's IE7 browser, Mozilla Firefox 2.0, and Opera all contain this type of anti-phishing measure. The screen below shows Google blocking a suspected phishing web site.


5. **Eliminating Phishing Mail -** Specialized spam filters can reduce the number of phishing emails that reach their addressees' inboxes. These approaches rely on machine learning and natural language processing approaches to classify phishing emails.

6. **Monitoring And Takedown** - Several companies offer banks and other organizations likely to suffer from phishing scams round-the-clock services to monitor, analyze and assist in shutting down phishing websites. Individuals can contribute by reporting phishing to both volunteer and industry groups, such as PhishTank.

## Legal Responses

1. **Goodin Convicted** - On January 26, 2004, the U.S. Federal Trade Commission filed the first lawsuit against a suspected phisher and Californian teenager Jeffrey Brett Goodin. He was the first defendant convicted by a jury under the provisions of the CAN-SPAM Act of 2003. He was found guilty of sending thousands of e-mails to AOL users, while posing as AOL's billing department, which prompted customers to submit personal and credit card information. He was sentenced to serve 70 months.

2. **In Brazil -** Phishing kingpin, Valdir Paulo de Almeida, was arrested for leading one of the largest phishing crime rings, which in two years stole more than $18 million.

3. **In the UK** - UK authorities jailed two men in June 2005 for their role in a phishing scam, in a case connected to the U.S. Secret Service Operation Firewall, which targeted notorious "carder" websites.

4. **In Japan -** In 2006 eight people were arrested by Japanese police on suspicion of phishing fraud by creating bogus Yahoo Japan Web sites, netting themselves 100 million yen ($870,000). The arrests continued in 2006 with the FBI Operation Cardkeeper detaining a gang of sixteen in the U.S. and Europe.

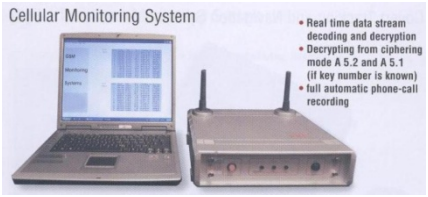
5. **Microsoft Attacks -** On March 31, 2005, Microsoft filed 117 federal lawsuits in the U.S. District Court for the Western District of Washington. The lawsuits accuse "John Doe" defendants of obtaining passwords and confidential information.

# Spy Stuff

# Chapter 38

**VME Spy Phone™ - Eavesdrop on Conversations From Anywhere in the World** - This product operates as a normal mobile phone where the holder can send and receive calls as usual. However, when you call the phone using a special access number, it automatically answers without any ringing or the holder being aware that you are connected to their phone in "listening mode". There will be no record of the call received from the special access number in the phone's list of received calls. There is also a proximity listening device enabling you to listen directly to what is going on up to five meters away from the phone.

**VME Cell Phone Interceptor** - Real time interception and tracking of cell phone communication* A proprietary technology allowing you to Intercept, follow, track and listen to communications using unique triangulation and other advanced technology. Active or Passive search and detection. Completely undetectable. Follow multiple targets simultaneously. Laptop size with extended range.




**The Picture Frame Bug**

This is a sneaky way to bug a room, a picture frame with a built in microphone that you can phone up and listen to what's going on.


**Tap your own phone line with Teleport 2.0**

### Cell Phone SIM Card Spy

This device allows you to recover deleted text messages from a cell phone. Just plug it in and erased messages on the phone are restored to the device, which you can read later by plugging it in to your computer.

### Under Door Remote Viewing Kit

The viewing kit allows you to see behind a door before you open it. The scope section is used to slide under the door and can fit in a space less then quarter of an inch. The field of view is 55° which can see from the floor right up to the ceiling. As well as seeing what it in the room, there is a right angle adapter which allows you to view the back of the door so you can observe any barricades or traps.

### MQ-1 Predator

The US Government has given the University of Michigan a $10 million dollar grant to come up with a “six-inch robotic spy plane modeled after a bat”.

### Honeywell Hovering Spy Drone

Spy drone that can fly a 100 waypoint flight plan at 57 MPH, at a 10,500 foot altitude. These Micro Air Vehicles (MAVs) are already in place over Iraq and Afghanistan. They are waiting for FAA permission to be used here in American soil. $???

**Spy Tie and the Concealed Camera Spy Pen** - is sure to blend in beautifully whilst keeping tabs on your co-workers or employees.

**The SpyCam Office Calculator**

This is a fully functioning electronic calculator complete with print roll, comes with a hidden 640 x 480 high resolution camera which, once armed via the units wireless remote control, will enter motion detection mode ensuring that the moment someone comes within range it will begin capturing video footage to an SD card concealed in a hidden compartment – with 2GB SD cards storing up to 128 hours of surveillance video. **$449**

**Estes Xb-30 Digital Camera Spy Plane**

A radio controlled digital camera spy plane with built-in digital camera that can take up to "26 aerial photographs" with the push of a button on the transmitter. Transferring the images to your computer via a USB port. Powered by electric fan engines with a wingspan of 55 in. and is 34 in. long.

**Shocking Suitcase**

Keep all your secret documents safe with this shocking suitcase -- 80,000 volts to be exact. The electric shock alarm is activated at the push of a button via remote control. A built-in secondary 107db alarm keeps would be thieves away. Available in brown or black colors.

### Shotgun Flashlight

A grenade-style pin removes the safety, and the flashlight fires a .410 shotgun round out the back when a button is pressed. A Mini-Mag size fires a .380 round.

### Listen To Conversations 15 Feet Away

Not your ordinary SL-65, this "Interceptor" version allows users to "dial up the device's super-secret number to instantly surreptitious listen in on whatever's happening up to five meters away from the mic." One drawback, it's priced at a whopping $2,155.


### Mouse Microphone

Keep a close ear on your computer with the CP-1. Hidden inside this otherwise normal looking mouse is a condenser microphone - capable of picking up on any nearby conversations. It measures 53 x 95 x 35 mm and weighs just 75g.

### Digital Camera Watch

Looks and works like a normal watch, however it can also take VGA digital photos! So when you are out and about, take some candid photos with your watch! Perfect at trade shows or even just out with your mates! The built in 2MB of memory is capable of storing up to 36 photos and it includes software and a serial cable (RS-232) for downloading images to a PC.


### Spy Glasses

They let you see who is behind you! The lenses on these spy glasses have a special coating that allows you to look straight ahead and still see what is going on behind you. Now, no one can sneak up behind you.

**Noise Amplifier**

The ultimate in surveillance equipment, this handy little device fits on the ear and uses a tiny amplifier to increase the level of ambient sound in a room. The sound is sent to the earpiece allowing the user to eavesdrop on conversations discretely.

**Key Shark - USB Keylogger**

Key stroke logging device which records every key pressed on a computer keyboard - storing an exact copy of everything typed by the user! With enough capacity to store half a million characters (key presses), it can quietly record the average computer user for many months and still have room to spare. Installation takes just seconds, and the KeyShark starts to record automatically. Key Shark works with USB style keyboards. It is a small external device, looking like and adapter plugged into a USB socket. **U.S. $ 280.95**

**Keyshark - PS/2 Port Keylogger**

The Keylogger is a device that can be connected to a keyboard to record all keystrokes and data entered. It is password protected, and offers a keyword search facility, enable/disable option, and will store over a years worth of data! Keyshark sits between the keyboard and your computer. **U.S. $ 280.95**

**Wrist Watch Digital Camera**

8M SDRAM allows storage of up to 26 VGA high resolution 350,000 pixel pictures. Auto exposure, auto white balance, edge detection with enhancement and back light compensation. Upload images to a Palm PDA, or PC. One AAA battery not included. Images are displayable on your PC in 16.7M (32-bit) color Comes with a USB wire link and a CD Rom so you can transfer and save the pictures into your computer. **U.S. $ 450.00**

### Tele Monitor 2000


Discreetly listen in on your premises via regular telephone lines from any telephone in the world! Requires no activating beeper or whistle and does not affect normal incoming and outgoing calls. Up to 4 units per line. Sensitive microphone will pick up even a whisper up to 35 feet away. To monitor, just dial your phone number from any tone telephone. Size : 5 1/2" x 3 1/2" x 1" This is a completely self-contained unit - no actual telephone required. It comes with modular plugs for instant connection to telephone jacks - needs no batteries. U.S. **$ 379.95**

### Super Ear


It increases your ability to hear the sounds around you - indoors and out. Spy on sensitive conversations. Hands-free listening, delivers a full 50+db of sound gain. Measures 3 1/2 x 1 3/4 x 3/4. Comes with earphones and binocular mounting - clip. U.S. **$ 78.95**

### Bug Detector


Modern day miniature "bugs" can be hidden anywhere. Listening devices can be easily planted in places like your office, residence, hotel etc. The Bug Detector not only tells if a bug is present, there are 3 LEDs: Level 1 (Weak), Level 2 (Medium), Level 3 (Strong), indicating the strength of the detected signal. You can zero-in on its exact location. From 50 Mhz to 3 Ghz , you choose to leave the bug or destroy it. All this can be done without alerting eavesdroppers. It can also detect wireless camera, wireless phone, wireless tap, and cell phones. Size: L 3.5" x W 2.1" Power: (AAA battery x 2) U.S. $ **239.95**

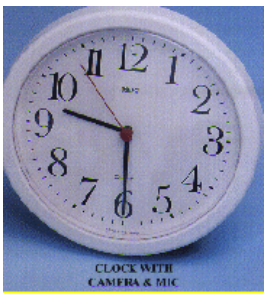
### Telephone Tap Detector

Instantly tells you if there is a tap or eavesdropper on the line. Automatically mutes your call if a tap is enabled while you are talking. U.S. **$ 269.95**

### Cellular Voice Encryption

The Cellular Voice Encryption snaps on to the dataport of an Ericsson cellular phone (included) working over the GSM network. It uses 256 Bit AES encryption algorithm which is the most advanced encryption standard for voice communication, even more advanced than the DES standard. Transparency operation, no action required by user. Military strength - offers voice protection against virtually all determined listeners. ** Price per unit - 2 units are needed (one at each side of the conversation). U.S. $ **2,200.00**

### Clock Camera



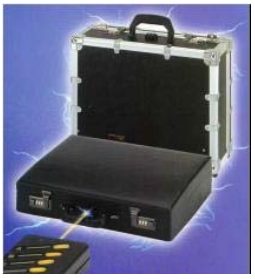

Clock Camera hides a wide angle lens behind the face - invisible no matter how hard you look! The camera has high resolution and has an electric iris for clear viewing in low light situations. The camera plugs in to a TV monitor or VCR. 12V power supply included. U.S. **$ 359.95**

### Key Chain - Alcohol Breath Analyzer

Breath Analyzer is a sensitive instrument measures breath alcohol content to equivalent blood alcohol content (BAC) within seconds. Shows 5 progressive key concentration levels denoted by a color coded LED display. **U.S. $ 149.00**

### 50,000 Volts Shocking Briefcase

The Remote Control Shocking Briefcase and Money Carrier, if it is picked up to 30 degrees out of its horizontal position, without being disarmed, the briefcase will give a 5 second 85dB warning siren and then shock the would-be thief at 50,000 volts of power. Also, when the briefcase is being carried, a thief may attempt to steal it, however with its' four function remote, you can allow the would-be thief to get well away from you, up to 500 ft. (well over the length of a football field) to avoid confrontation and then... press the remote control key to shock them with 50,000 volts !! **$ 699.00**



### Dummy Security Video Camera

Authentic looking camera simulates a high tech security system and makes crooks think twice. Flashing red LED fools unwanted visitors into thinking they are being watched. Uses 2 AA batteries. U.S. **$ 39.95**


### Mini Night Vision

The world smallest night vision unit with a built-in infrared illuminator. You will see even in total darkness! Good for spying. Measures 5-1/4 x 2- 1/2 inches. 1.6 x magnification. Amplifies light 15,000 times. Comes with carrying case. Requires AAA batteries. U.S. **$ 435.95**

### Cobra Vision

These goggles were originally developed for Soviet Air Force pilots who required hands-free night vision. Helicopter pilots, paratroopers and tact-ops commandos also use them. They amplify light 20,000 times. Infrared illuminator allows you to see in total darkness. Wide, 36 deg. field of view. Adjusts to fit any size head. Dust, shock and water-resistant. U.S. **$ 795.95**

### The Truth Machine

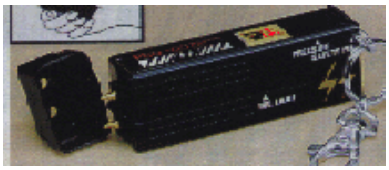
Pocket-sized device that monitors the truth behind someone's words by responding to voice changes and inflections. The device is equipped with a highly sophisticated program and computer chip that allow it to work on the same principle as a lie detector. It is extremely sensitive to stress and subtle changes in voice inflection as an indicator of truthfulness. U.S. **$ 89.95**

### Acoustical Jammer

Secure your room conversation. It works by generating unfilterable random white noise. This desensitizes any microphone - based eavesdropping. The Jammer also protects you from tape recorders, shotgun mics, wired devices, microwave and laser pickups. **U.S. $275**


### Mini Stun Gun

The world's smallest stun gun (the size of a pack of gum). It has enough juice to stun a 300lb. attacker without permanent damage. Simply touch the attacker's skin or clothes to deliver a 400 volt charge! Attach to belt or key ring, safety pin prevents any accidental discharge. **U.S. $ 43.95**



### Pro Track 1

Digital Vehicle Tracking System. Tracking range about 3 miles. Digitally encrypted signaling (confidential to owner). Displays ID code of your target transmitter. Simultaneous monitoring of up to 10 targets. Displays distance to target in feet (from 75 to 65,000) Available optional transmitters: Magnet Mount Vehicle Tracker, Body Transmitter, Belt Clip Transmitter, Child monitoring (kidnap) Transmitter. U.S. **$ 2,850.00**

### Peephole Reverser

Developed to assist law enforcement officials to assess potential threats or activity behind closed doors, these units are now available to the public. Simply place the lens over the peephole and you can see into the room without alerting anyone inside by negating the peephole's lens. Length: 2.7" weight: 1.5 oz. U.S**. $ 89.95**

### Spy Phone


It may look like a regular Nokia Cellular phone, however this Super technology goes beyond its standard capabilities. It operates as a normal cellular phone - but when the phone is called in on a special "Spy" mode (from anywhere in the world) it will automatically answer without any ringing or lights coming on and the display stays the same as if it is on a "Standby Mode". While on the "Standby mode" it will pickup the sounds nearby and transmit them back to you (the caller). All you have to do is to activate it as if you would activate any cellular phone. Talk Time: 3 to 4 Hours. Standby Time: up to 6 Days. Weight: 2.8 oz. Technology: GSM standards for U.S. - Europe - Asia.

NOTE : Except for Law Enforcement, this item is not available to U.S. residents. U.S. **$ 2,400.00**

### Micro UHF Room Transmitter

Transmitter - This powerful little device has a 5 day battery life and can be concealed almost anywhere. It will pick up the slightest whisper from up to 40 feet away and transmit to our UHF receiver with amazing clarity up to a distance of 600 meters. - Dimensions: 6.5 cm. x 3 cm. x 1 cm.

Receiver - About the size of a cigarette pack, this is a state of the art two channel UHF receiver. Recently upgraded, its' sensitivity is incredible. It is capable of receiving the signal from our UHF transmitter for long range use with amazing clarity. A recorder can be connected to the receiver so the user can record all conversations and listen, too.

Please note this item is NOT available to U.S. residents U.S.
**$ 1,370.00**

### Envelope X-ray Spray

Envelope X-RAY Spray turns opaque paper temporarily translucent, allowing the user to view the contents of an envelope without ever opening. 30 seconds after application, the envelope will return to its' original state, leaving absolutely no markings, discoloration or other indications of use. Each can treats several hundred square inches. Non-flammable, non-conductive and non-photochemically reactive. Environmentally-friendly (contains no Freon). Net weight: 8 oz. WARNING: Not to be used on U.S. Mail, except by or with the express permission of the addressee. Cannot ship by Air. U.S.
**$ 45.95**

### Air Taser

The AIR TASER is a small handheld self-protection system which utilizes compressed air to shoot two small probes up to 15 feet away. These probes are connected by wire to the launcher which sends a powerful electric signal into the nervous system of an assailant. This causes the body to go limp as the brain loses control over the rest of the body. The TASER is highly effective because the electrical signal penetrates the nervous system regardless of the placement of the probes. **U.S. $ 395.95**

### Fiber Optic Snake Camera

Snorkel Camera Tube Camera, Spy Camera, all in one. The remote head of this color video camera is the smallest on the market, measuring only .29" in diameter and 1.4" in length, comes with a micro 3.9mm lens. Optional built in light source (measures .55" diameter and 4" in length). The remote head is connected to the miniature control unit by a 38" super flexible cable. Great for surveillance under the door, tight places, machine vision, robotics, and quality control. **US $1,398**


### Hidden Camera

Smoke Detector Camera hides a wide angle lens behind the face plate. Totally invisible no matter how hard you look! High resolution with electric iris for clear viewing in low light. It also contains a hidden microphone for audio. Comes with 12V power supply, and high ceiling mount. Wireless or wired, color or B&W camera, your choice. **US $389.95 wired, $689.95 wireless.**

**MOBIL TRACK**

Monitor detailed information about a vehicle's travel activities using a satellite positioning network (GPS) cross referenced with digital street maps providing proof of exact date, time, speed, and location right down to the street level. US **$2,495**

**Telephone Voice Changer**


The Telephone Voice Changer incorporates an eight-level pitch adjustment. At the high range a man's voice will sound like a woman. At low range a woman will sound like a man. A built-in amplifier can increase the sound of the incoming voice. It installs by plugging in to the base and handset of the telephone. **US $59.95**

**UV Pen**

The ink in this pen is invisible to the naked eye, so any paper you write on will appear to be blank. However, under a UV light source, your "secret message" will appear. Possible technique for securing passwords without leaving them visible in workspace area. US **$5.95**

**Cellular Blocker**


The systems utilize a unique transmission method that confuses the decoding circuits of cellular handsets as if no cellular base station is within the service area. Upon activating the Blocker, all idle phones will indicate "NO SERVICE". Consequently, all cellular phone calls already in progress within the defined area will be cut-off and the radio link will be lost. **US $1,948**

# Privacy Test

# Chapter 22

**Privacy Test**

As usage of the Internet and CRM products expand, huge amounts of data are being collected on everyone. With each bulging database comes the increased possibility that tender information will fall into the wrong hands or that erroneous information will be collected. Everywhere you turn cameras are watching you, companies are building profiles on you and your habits, software programs track where you go and what you read on the Internet. The public has pushed back with many people crying enough is enough. This web page addresses some of the privacy issues and some of the measures you can take to protect yourself at least a little. However please be advised that this web site does not pretend to address all of the issues or solve the privacy dilemma. You alone are responsible for enacting privacy measures which are consistent with your own desires for privacy.

**Take the Privacy Test**

1. Have you ordered your own credit reports for $8.00 each?

| | | |
|---|---|---|
| **www.experian.com** | Yes | No |
| **www.equifax.com** | Yes | No |
| **www.transunion.com** | Yes | No |

2. Have you ordered your medical history report for $8.50? Yes No

**www.mib.com**

3. Have you ordered your own Social Security Earnings report for free? Yes No

**www.ssa.gov**

4. Have you ordered a copy of your driving record? Yes No

http://www.ark.org/dfa/motorvehicle/driverservices.html

| | | |
|---|---|---|
| 5. Do you take time to "Opt Out" of junk mail? | Yes | No |

http://www.the-dma.org/

| | | |
|---|---|---|
| 6. Do you avoid filling out warranty and registration cards - or use an alias when doing so? | Yes | No |
| 7. Do you avoid publicly donating money to charities? | Yes | No |
| 8. Do you avoid joining clubs and organizations? | Yes | No |
| 9. Do you avoid subscriptions to magazines or use an alias? | Yes | No |
| 10. Do you have an un-published telephone number? | Yes | No |
| 11. Do you avoid sweepstakes? | Yes | No |
| 12. Do you avoid giving out your social security number whenever possible with persistence? | Yes | No |
| 13. Do you refuse to allow your credit card number to be written on your checks? (unlawful in many states to do so) | Yes | No |
| 14. Do you refuse to allow your phone number and address to be written on your credit card slips? (also unlawful in many states) | Yes | No |

| | | |
|---|---|---|
| 15. Do you avoid cordless phones? | Yes | No |
| 16. Do you avoid cellular phones? | Yes | No |
| 17. Do you subscribe to "Caller ID Blocking"? | Yes | No |
| 18. Do you have a PO Box address to use in all but the most important circumstances? | Yes | No |
| 19. Do you shield your hand at ATM machines when entering your PIN number? | Yes | No |
| 20. Do you shield your hand when entering calling card numbers at public telephones to make long distance calls? | Yes | No |
| 21. Do you read the fine print on applications and order forms? | Yes | No |
| 22. Do you encrypt your e-mail? | Yes | No |
| 23. Do you use a combination of letters and numbers in your passwords? | Yes | No |
| 24. Do you change your passwords occasionally? | Yes | No |
| 25. Do you use different passwords for every account? | Yes | No |

| | | |
|---|---|---|
| 26. Is your computer password protected at the system level? | Yes | No |
| 27. Do you have a second e-mail account for personal use? | Yes | No |
| 28. Do you have a second e-mail account that you use for less important purposes? | Yes | No |
| 29. Do you sign your name legibly when signing Signature Capture Devices? | Yes | No |
| 30. Do you read privacy policies on web sites? | Yes | No |
| 31. Have you taught your children not to give out personal information on the internet? | Yes | No |
| 32. Do you clear your cache frequently after browsing? | Yes | No |
| 33. Do you make sure to use secure connections when transmitting sensitive data over the internet? | Yes | No |
| 34. Do you reject un-necessary cookies? | Yes | No |
| 35. Do you use anonymous re-mailers when appropriate? (Hushmail for example) https://www.hushmail.com/ | Yes | No |
| 36. Do you use anonymizers when browsing? http://www.anonymizer.com/ | Yes | No |

| | | |
|---|---|---|
| 37. Do you use a personal firewall on your internet connection? | Yes | No |
| 38. Have you read your company's privacy policy? | Yes | No |
| 39. Do you perform due diligence on any new service, company, or web site that you patronize? | Yes | No |
| 40. Do you avoid using newsgroups or chat rooms, or at least use an alias? | Yes | No |
| 41. Do you use a digital ID to authenticate your e-mail? | Yes | No |
| 42. Do you ignore junk e-mail? | Yes | No |

**How did you score?**

Multiple Your **YES** responses by 3. In previous audience surveys, the audience has scored on average as follows:

Less than 20 - 27%;

20 to 40 - 55%;

40 to 60 - 8%

(10% did not report their score.)

The higher you score, the more measures you have taken to protect your privacy.


# Fake IDs

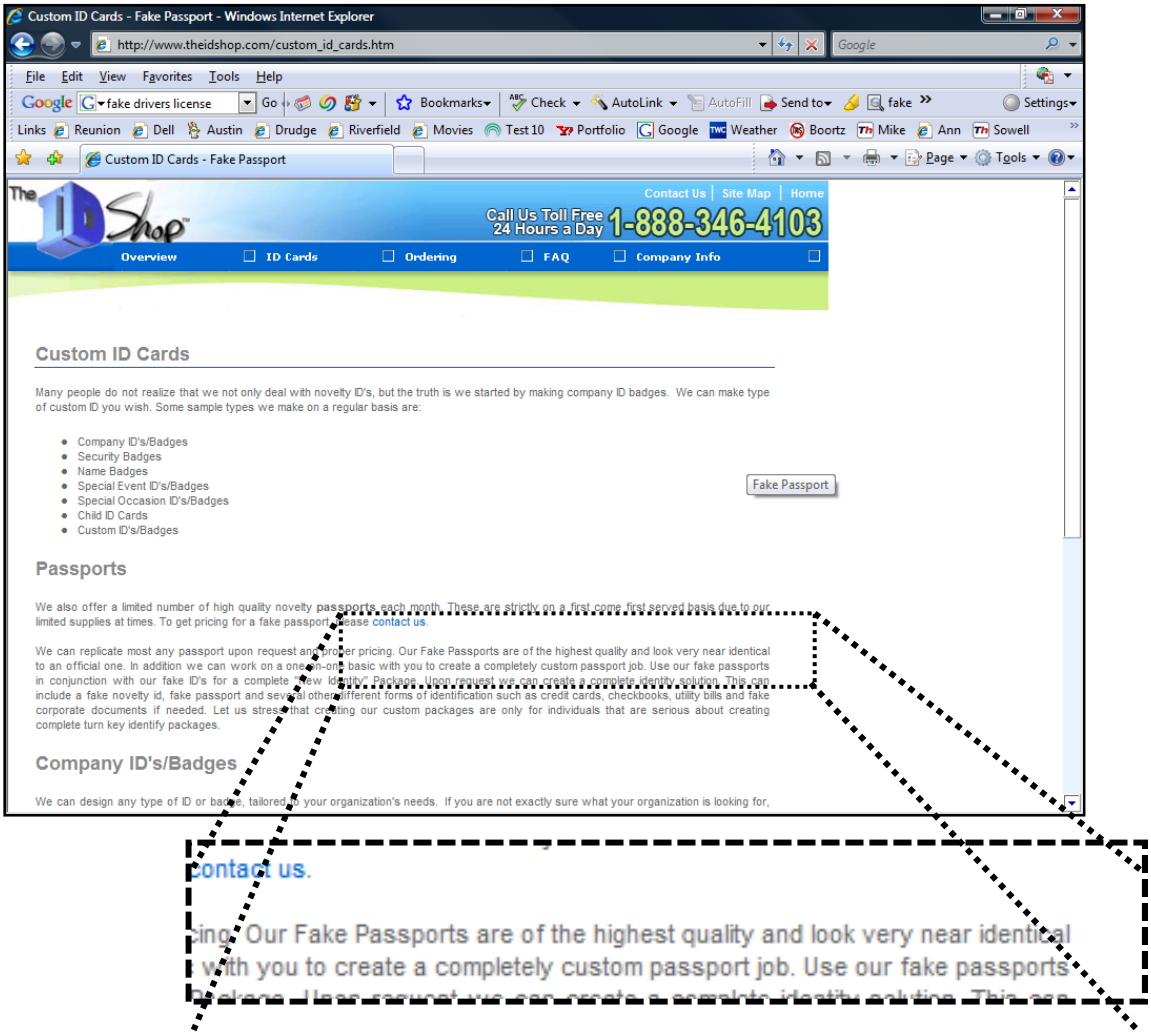
# Chapter 23

## Do-it-Yourself Fake IDs

For many years the graphic images needed to create your own driver's license for each state were freely available for download from numerous web sites. As a result, millions of computer-savvy teenagers have created fake driver's licenses despite the holograms and other high-tech security features that states now put on licenses to thwart forgers. Using the Internet, anyone willing to break a few laws can be a mass producer of fake IDs. Fake licenses can be made easily by downloading these templates, scanning a picture into the computer, editing the template and printing the finished product with a photo-quality inkjet printer. Since 9/11, many of these sites have been shut down  but new sites pop up continuously.

## Are Fake ID's Harder to Obtain?

There are over 900,000 web sites offering to help you obtain a fake ID. These services offer holograms, full color photos, professional laments, and all the trimming to make a fake ID. For example, this web site for "The ID Shop" claims to provide "near identical" passports.

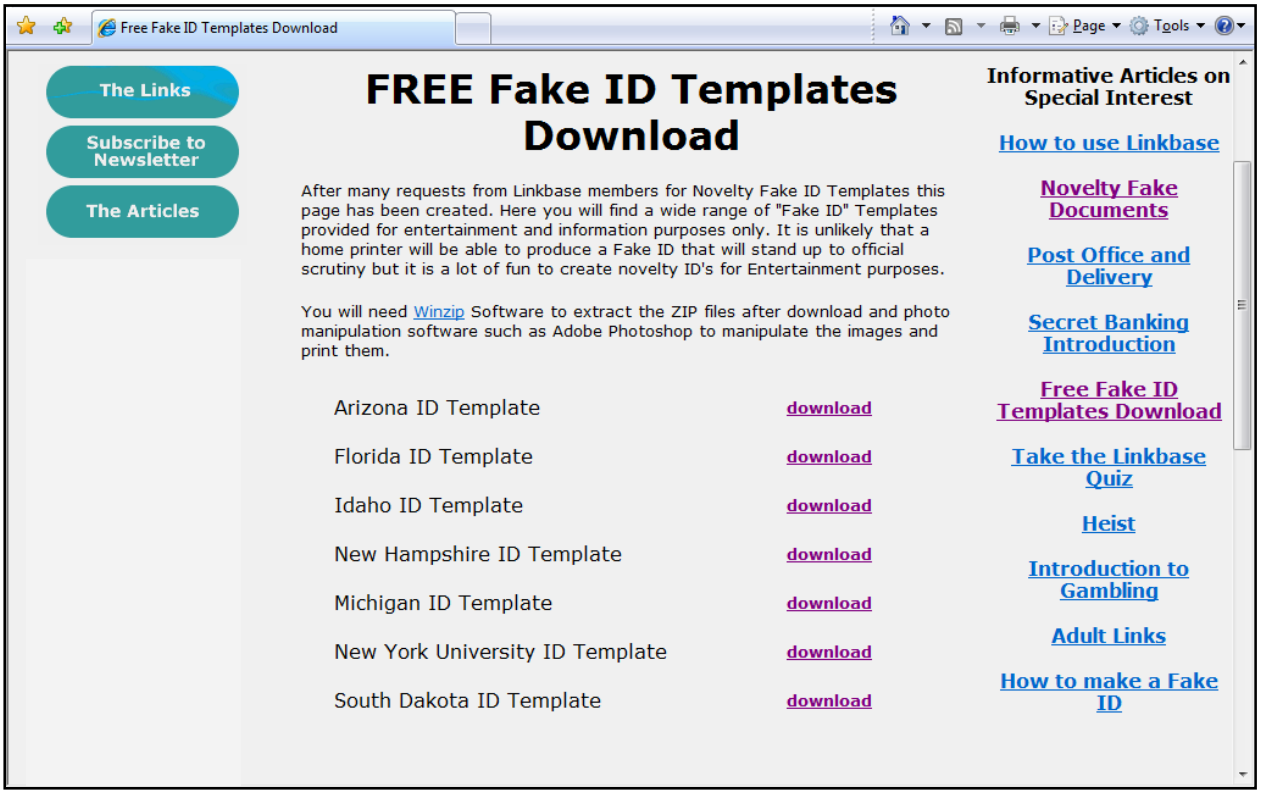


In years past there were no procedures for verifying the authenticity of an ID – only the police had that capability. However today, online verification terminals are popping up everywhere. Further the laws are different now, for example today just handing a fake ID to a bar bouncer could land you in jail.

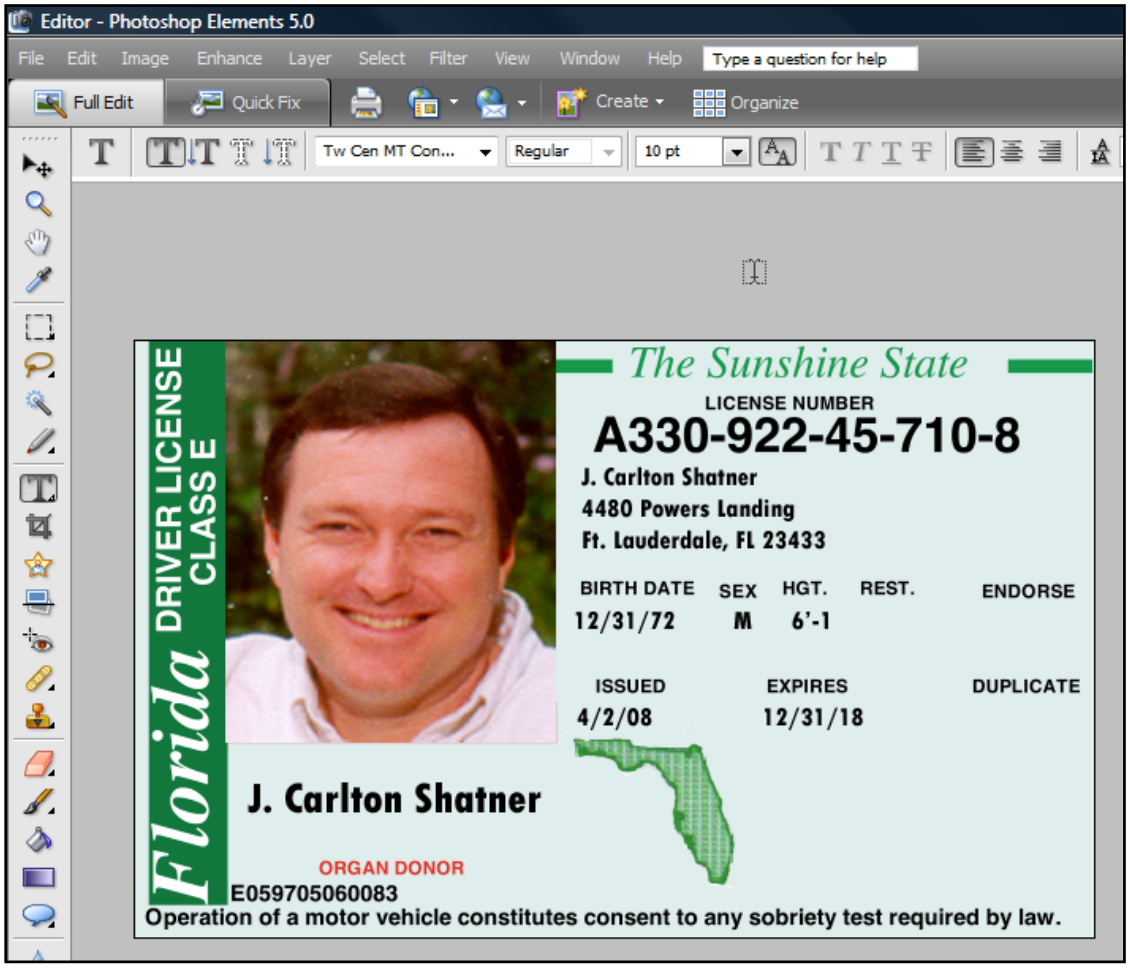
Some reports indicate that it is actually fairly difficult to get your hands on high-quality fake IDs today. They claim that most of those enticing fake ID sites on the internet are total rip-offs that deliver nothing, or they deliver poor quality IDs with the word "Novelty" stamped on the back. Some fake ID sites promise to deliver fake drivers licenses, but when your license arrives it's a worthless go-kart license. They get away with this because whom can you complain to?

While there are numerous Fake ID web sites on the Internet now, most do not seem to offer actual replica driver's licenses or other official government documents. I can only conclude that the Department of Homeland Security is monitoring the Internet and taking measures to shut down these operations, or at least preventing them from producing official looking government issued IDs.

However, they are not doing a good enough job. In less than 10 minutes of searching, I found the following web site that allowed me to download driver's license templates for Florida, Michigan, Arizona, New Hampshire, Idaho, New York, and South Dakota.




I was able to edit these templates in PhotoShop in about 5 minutes to create the following fake ID using my picture and fake information.




Now I only need to print it out and apply a transparent lament sheet and trim to produce the fake ID. The numbers and information contained on the ID won't match the data in the Florida database, but this ID would probably be good enough to enable under-aged drinking, or fool a doctor's office into admitting a person and providing services, to engage in a number of other crimes.

## Algorithms

Today most states use some type of algorithm to make duplication of driver's licenses harder to achieve. For example, in Georgia, the last digit in the year of birth also appears elsewhere on the drivers license in an inconspicuous place – if the numbers do not match, the ID is obviously a fake ID. Forgers who are not aware of this check have only a 10% chance of producing a drivers license that will pass close inspection.

## Outside the Internet, Fake IDs Seem to be Easy to Obtain

Despite the fact that many fake ID web sites may seem to be closed for business, it appears that there are other sources for high quality fake IDs other than the Internet. From my own personal experience I know a friend who's daughter went to college in 2007 and during her first sorority meeting, applications and fees for fake IDs were solicited at. The resulting IDs were high quality – like this fake ID shown below.


*(A $100,000 identity theft and check fraud scam was perpetrated by this thief using this phony driver's license in Oregon State, targeting construction related businesses.)*

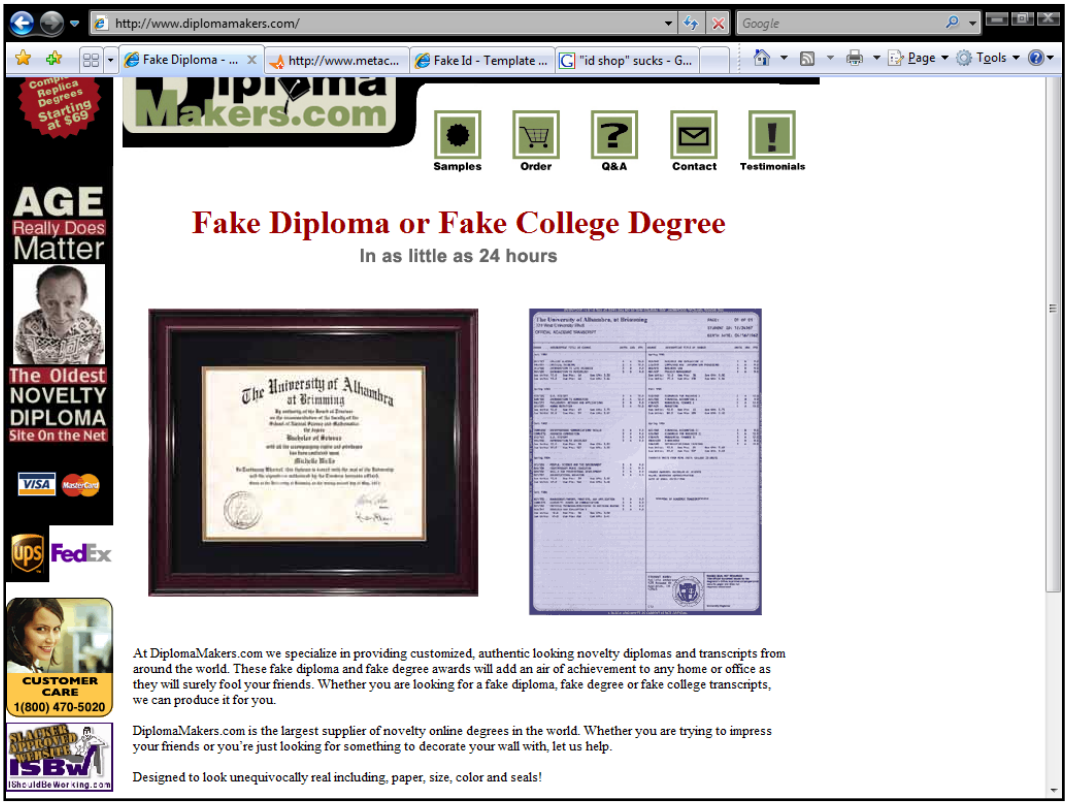
Congressional investigators confirmed this when they easily convinced motor vehicle agency employees around the country to issue genuine drivers licenses. According to a report from the General Accounting Office, agents operating undercover in seven states and the District of Columbia, ultimately obtained drivers licenses at every agency where they applied. The most serious vulnerabilities appeared in California, where agents managed to complete the process to receive three temporary state driver's licenses within two days using the same fake information.

Florida police also confirm the availability of fake IDs. During four spring-break weeks, Florida police staked out bars, restaurants and nightclubs in Panama City and Daytona Beach. The police looked for IDs with flawed holograms and incorrect letter and number codes that are supposed to be known only by police and a state's motor vehicles department.

They arrested about 350 teenagers for carrying fake IDs and 1,200 for underage drinking and confiscated 10,000 bogus IDs. That's an indication, police said, of the enormous popularity of counterfeit licenses among high school and college students. If you extrapolate the Panama City and Daytona Beach figures, he says, "you're talking millions and millions" of fake IDs around the country. Another police officer estimated that 50% of underage high school and college students have fake IDs.

## Fake Diploma's, College Degrees & Other Documents

Fake diplomas and college degrees including fake transcripts also seem to be readily available as this web site shows.



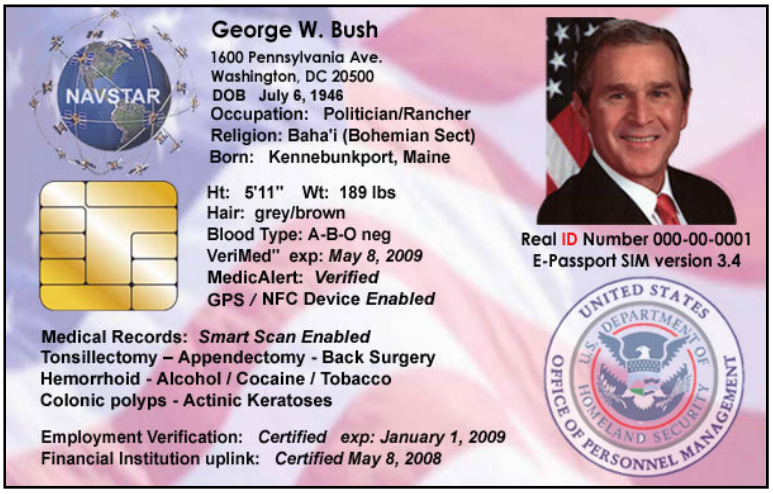

In fact there are many internet sources for many fake documents from Fake High School Diplomas, Fake transcripts, fake birth certificates, fake business cards, fake ID badges, etc.

## The Solution – Background Checks

The solution to the threat of fake IDs is rather simple – do background checks on everybody you come in contact with – including customers, suppliers, employees and subcontractors. Don't give anybody access to your building, your operations, or your data until you confirm who they are. As an example, Net Detective claims that you can search over 3.1 billion records to obtain Information on over 90% of residents in the U.S. They claim to have 843,000 users. They provide instant access, no download is required. The information provided includes criminal records, family history, birth, death, social security, adoption, DMV Records, unlisted phone numbers, address, phone number, e-mail Addresses, access to your own credit reports, and your own FBI file.


## Key Points

1. Fake ID and drivers license templates are available on the web.
2. Many fake ID web sites provide poor quality IDs, GoKart IDs, or NOVELTY IDs.
3. At least one sorority solicits money for fake IDs at their first chapter meetings.
4. Codes and algorithms are used to help prevent drivers license forgeries.
5. Fake diplomas and college transcripts are also available.
6. A background check is your best protection against fake IDs.
7. ID authentication methods and web sites are becoming more prevalent.
8. Today, the best fake IDs are backed up by a real identity using identity theft.




# National ID Cards

# Chapter 24

National ID cards are advocated by some as a means to enhance national security, unmask potential terrorists, and guard against illegal immigrants. They are already in use around the world including most European countries, Hong Kong, Malaysia, Singapore and Thailand. The United States and United Kingdom continue to debate the merits of adopting national ID cards.

Historically, Americans have rejected the idea of a national ID card. When the Social Security Number (SSN) was created in 1936, it was meant to be used only as an account number associated with the administration of the Social Security system. Though use of the SSN has expanded considerably, it is not a universal identifier and efforts to make it one have been consistently rejected. For example:

1. In 1971, the Social Security Administration task force rejected the extension of the Social Security Number to the status of an ID card.

2. In 1973, the Health, Education and Welfare Secretary's Advisory Committee on Automated Personal Data Systems concluded that a national identifier was not desirable.

3. In 1976, the Federal Advisory Committee on False Identification rejected the idea of an identifier.

4. In 1977, the Carter Administration reiterated that the SSN was not to become an identifier.

5. In 1981 the Reagan Administration stated that it was "explicitly opposed" to the creation of a national ID card.

6. The Clinton administration advocated a "Health Security Card" in 1993 and assured the public that the card, issued to every American, would have "full protection for privacy and confidentiality." Still, the idea was rejected and the health security card was never created.

7. In 1999 Congress repealed a controversial provision in the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 which gave authorization to include Social Security Numbers on driver's licenses.

In response to the tragic events of Sept. 11, 2001, there has been renewed interest in the creation of national ID cards. Soon after the attacks, Larry Ellison, head of California-based software company Oracle Corporation, called for the development of a national identification system and offered to donate the technology to make this possible. He proposed ID cards with embedded digitized thumbprints and photographs of all legal residents in the U.S. There was much public debate about the issue, and Congressional hearings were held. Former House Speaker Newt Gingrich testified that he "would not institute a national ID card because you do get into civil liberties issues." When it created the Department of Homeland Security, Congress

made clear in the enabling legislation that the agency could not create a national ID system. In September 2004, then-DHS Secretary Tom Ridge reiterated, "The legislation that created the Department of Homeland Security was very specific on the question of a national ID card. They said there will be no national ID card."

The public continues to debate the issue, and there have been many other proposals for the creation of a national identification system, some through the standardization of state driver's licenses. The debate remains in the international spotlight - several nations are considering implementing such systems. The U.S. Congress has passed the REAL ID Act of 2005, which mandates federal requirements for driver's licenses. Critics argue that it would make driver's licenses into de facto national IDs.

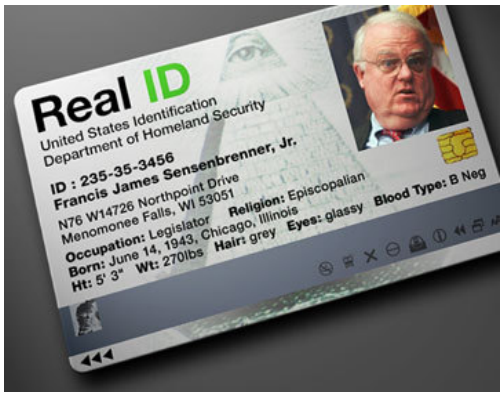
### The REAL ID Act of 2005

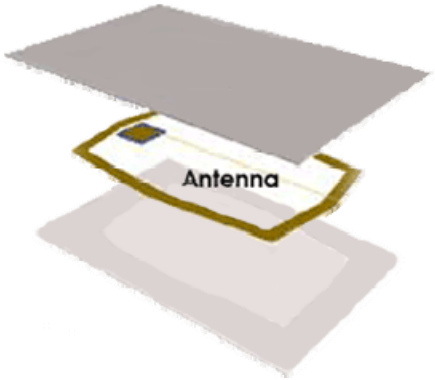
The REAL ID Act of 2005 is a law which imposes federal technological standards and verification procedures on state driver's licenses and identification cards, many of which are beyond the current capacity of the federal government, and mandating state compliance by May 2008. As of April 2, 2008, all 50 states have either applied for extensions of the original May 11, 2008 compliance deadline or received unsolicited extensions, meaning that the REAL ID Act will not become an issue at federal facilities and airports until December 31, 2009.

Some claim that REAL ID turns state DMV workers into federal immigration officials, as they must verify the citizenship status of all those who want a REAL ID-approved state driver's license or identification cards.

In order to get a Real ID you will be required to show your birth certificate, proof of address and citizenship, photo ID, and Social Security cards which are just some of what you might be asked to present to the DMV. If you enter an establishment and are required to show your Real ID all of your personal information can be scanned and digitally stored from the RFID or strip on your card, such as your: name, birth date, sex, ID number, a digital photograph (Notice that the image above also shows the individuals religion. Why would the DHS want to know your religious beliefs?)

Homeland Security may also add additional requirements — such as a fingerprint or retinal scan — they won't issue their specifications for the Real ID for several months. The Department of Homeland Security is in charge of the Real ID and each card will have personal data encoded on a strip and/ or a RFID chip. DHS contemplates using the REAL ID system as part of its Federal border security program and requested comments on how States could incorporate long-range radio frequency identification ("RFID") technology into the REAL ID card so that it could be used as part of the Western Hemisphere Travel Initiative.




Revelation 14:9-11


# Fake Social Security Cards

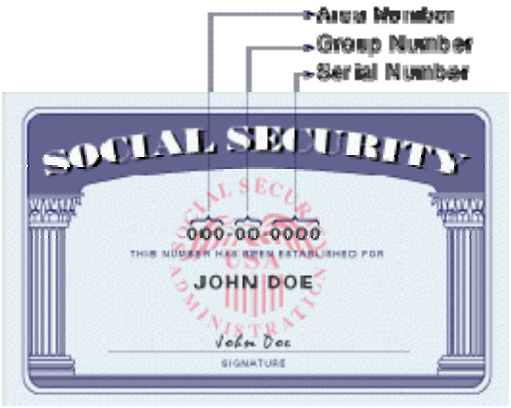
## Chapter 25

## Social Security Cards Are Required

The US federal government requires all legal residents to have a valid social security card. This card is used by the Internal Revenue Service (IRS) to track of an individual's earnings and taxes.

## The Social Security Number

The digits in the Social Security Number are divided into three parts:




1. **The Area** - The first three digits of a social security number are based on an algorithm applied to the recipient's ZIP Code (based on the mailing address shown on the social security application). The following table shows how area numbers have been assigned.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 001-003 | New Hampshire | 261-267 | Florida | 449-467 | Texas | 530 | Nevada |
| 004-007 | Maine | 589-595 | | 627-645 | | 680 | |
| 008-009 | Vermont | 766-772 | | 468-477 | Minnesota | 531-539 | Washington |
| 010-034 | Massachusetts | 268-302 | Ohio | 478-485 | Iowa | 540-544 | Oregon |
| 035-039 | Rhode Island | 303-317 | Indiana | 486-500 | Missouri | 545-573 | California |
| 040-049 | Connecticut | 318-361 | Illinois | 501-502 | North Dakota | 602-626 | |
| 050-134 | New York | 362-386 | Michigan | 503-504 | South Dakota | 574 | Alaska |
| 135-158 | New Jersey | 387-399 | Wisconsin | 505-508 | Nebraska | 575-576 | Hawaii |
| 159-211 | Pennsylvania | 400-407 | Kentucky | 509-515 | Kansas | 750 | |
| 212-220 | Maryland | 408-415 | Tennessee | 516-517 | Montana | 751 | |
| 221-222 | Delaware | 756-763 | | 518-519 | Idaho | 577-579 | District of Columbia |
| 223-231 | Virginia | 416-424 | Alabama | 520 | Wyoming | 580 | Virgin Islands |
| 691-699 | | 425-428 | Mississippi | 521-524 | Colorado | 580-584 | Puerto Rico |
| 232-236 | West Virginia | 587 | | 650-653 | | 596-599 | |
| 232 | North Carolina | 588 | | 525,585 | New Mexico | 586 | Guam |
| 237-246 | | 752-755 | | 648-649 | | 586 | American Samoa |
| 681-690 | | 429-432 | Arkansas | 526-527 | Arizona | 586 | Philippine Islands |
| 247-251 | South Carolina | 676-679 | | 600-601 | | 700-728 | Railroad Board** |
| 654-658 | | 433-439 | Louisiana | 764-765 | | 729-733 | Enumeration at Entry |
| 252-260 | Georgia | 659-665 | | 528-529 | Utah | | |
| 667-675 | | 440-448 | Oklahoma | 646-647 | | | |

Social Security numbers containing area numbers other than those found on the table above are impossible.

Prior to 1972, cards were issued in local Social Security offices around the country and the Area Number represented the location from where the card was issued (the numbering scheme was designed in 1936 (before computers) to make it easier for SSA to store the applications in our files). In 1972, SSA began assigning SSNs and issuing cards centrally from Baltimore; and the area number assigned is based on the recipient's ZIP code. Since the applicant's mailing address does not have to be the place of residence, the Area Number does not necessarily represent the State of residence. However, generally speaking, area numbers have been assigned beginning in the northeast and moving westward. So people on the east coast have the lowest numbers and those on the west coast have the highest numbers.

2. **The Group -** The middle two digits range from 01 to 99 but are not assigned in consecutive order. For administrative reasons, group numbers issued first consist of the ODD numbers from 01 through 09 and then EVEN numbers from 10 through 98, within each area number allocated to a State. After all numbers in-group 98 of a particular area have been issued, the EVEN Groups 02 through 08 are used, followed by ODD Groups 11 through 99.

   Because this numbering scheme is confusing and since the application form for an SSN asks for identifying information such as date of birth, place of birth, parents' names, and (optionally) the applicant's race, a common myth is that the group ID identifies the cardholder by a specific group – such as race. According to the SSA, this is not true.

3. **Serial Numbers** - The last four digits run consecutively from 0001 through 9999.

## Obtaining Fake Social Security Cards

According to an article in the Arizona Republic, within hours of crossing the border, illegal immigrants can buy them from "runners" on virtually every street corner. "Mica, mica," runners brazenly say to potential customers. Mica (pronounced MEE-ka) is Spanish slang for the green cards. Other dealers are more discreet as they pass out business cards for auto mechanics, yard work, taxi cabs and other services that are really fronts for makers of fraudulent documents.

Edward Ochoa is an undercover investigator who buys fake documents as part of the Arizona Fraudulent Identification Task Force. He explains how the process of obtaining a fake social security card, green card, or drivers license works. To get a fake ID, a buyer provides a passport photo then waits while a runner takes the image to a "manufacturer," usually another undocumented immigrant holed up in an apartment nearby. If they don't have a photo, the runner can usually take a picture with an instant camera. Reportedly, a "two-pack" - a green card and a Social Security card - costs as little as $70 on the street. A "three-pack" - a green

card, driver's license and Social Security card - goes for $140 to $160. Those prices buy documents with randomly generated numbers. Sometimes the numbers invented by a manufacturer coincidentally belong to actual people.

Buying fake documents made with government-issued ID numbers and a matching name stolen from someone else is far more expensive. Those documents are more difficult to get and cost three to five times as much as ones using bogus Social Security and immigration numbers. Some numbers are stolen. Others belong to children or to people who died.

## Making Fake Social Security Cards

Templates of driver's licenses, green cards and other documents can be bought on the black market, downloaded from the Internet or produced from scratch with a graphics software program. Producing fraudulent documents has become much easier all you need is a computer, scanner, a graphics software program like PhotoShop, and high-grade card printer like the ones shown below. They cost about $1,000 and print on plastic or PVC blanks. Card blanks cost about $1.00 each.

Within two hours of taking an order for fake documents, the runner returns with documents real enough to fool unsuspecting employers or to satisfy unscrupulous ones.

## Social Security Card Security Features

1. The card contains a blue tint marbleized random pattern. Any attempt to erase or remove data is easily detectable because the tint is erasable.

2. Small multi-colored discs are randomly placed on the paper stock and can be seen with the naked eye.

3. Intaglio printing of the type used in US currency is used for some printing on the card and provides a raised effect that can be felt.

By today's standards, these security features are considered lame. Because Social Security cards are paper, many people laminate their cards. However, a laminated card can hamper the ability of the government to utilize these security features. The government will replace your card free if in case you lose it.

## Stronger Social Security Cards on the Way

Congressmen introduced legislation in February 2008 to enhance the security features of Social Security cards. The proposed new cards will feature:


1. A photograph
2. A fingerprint
3. A computer chip
4. A bar code
5. A magnetic strip

The cards would be modeled after the Common Access Card issued by the Department of Defense, mostly to active military reserve members and their dependents, said U.S. Rep. Mark Kirk (R-Ill.), a sponsor of the bill. Current Social Security cards have limited security features and have no photo or biometric data, he said.

## Lose Your Business Hiring Illegal's

In July, 2008 Arizona enacted a tough employer-sanctions law which revokes business licenses of employers caught knowingly hiring illegal workers a second time. It also requires the more than 150,000 licensed Arizona employers to run Social Security numbers and other data for new employees through the federal Basic Pilot Program, an electronic verification system. Two other states, Colorado and Georgia, have passed similar laws.

# Identity Theft

## Chapter 26

## Identity Theft

According to U.S. Federal Trade Commission report, it is estimated that more than 50 million Americans were victims of identity theft. About half of the victims knew how their identity was stolen. The report found evidence that suggests that quick discovery of identity theft reduces the risk of thieves opening unauthorized accounts. Here are some relevant statistics:

1. Accounts were opened in 45 percent of identity theft cases in which at least six months elapsed before victims noticed their information was misused. Accounts were opened in fewer than 10 percent of cases where victims learned of misuse within a month.
2. 33.4 million Americans were victims of identity theft from 1990 to 2003.
3. 34% say someone obtained their credit card information, forged a credit card in their name, and used it to make purchases.
4. 12% say someone stole or obtained improperly a paper or computer record with their personal information on it and used that to forge their identity.
5. 11% say someone stole their wallet or purse and used their identity.
6. 10% say someone opened charge accounts in stores in their name and made purchases as them.
7. 7% say someone opened a bank account in their name or forged checks and obtained money from their account.
8. 7% say someone got to their mail or mailbox and used information there to steal their identity.
9. 5% say they lost their wallet or purse and someone used their identity.
10. 4% say someone went to a public record and used information there to steal their identity.
11. 3% say someone created false IDs and posed as them to get government benefits or payments.
12. 16% say it was a friend, relative or co-worker who stole their identity.
13. The seven million victims the survey identified in 2002 represent an 81% rise over victims in 2001.

Security risks related to identity theft are on the rise. There are a number of ways in which identity thieves could threaten your computer systems. For example, they could use employee badges to enter your premises, or masquerade in the community as your employee or vendor. For example, a thief might assume the identity of a vendor's sales representative and visit your accounts payable department to collect cash or check payments. With today's technology, it is

easy to reproduce business cards, badges, uniforms and even vehicle identification. That same thief might masquerade as one of your employees and attempt to withdraw money from your corporate bank accounts. An identity thief could republish your web site to a similar domain name, and change only the contact information. The possibilities are frightening.

To protect against identity fraud, common sense is your best ally. Some of the top prevention measures include the following:

1. Setting up PIN numbers on all bank accounts
2. Using finger print or retina scan technology instead of passwords and badges to prevent access to computer systems or buildings
3. Instruct employees not to write passwords down
4. Force users to change passwords monthly
5. Safeguard employee information such as social security numbers or employee numbers from non-authorized personnel
6. Use shredders to destroy sensitive documents
7. Reconcile all statements timely to the penny
8. Password protect all traveling laptops at the system level.
9. Have someone in your organization to search the internet for the use of your corporate name or the names of key individuals regularly to protect against improper use.

Another key threat from identity theft is that of hiring a masquerading employee. Using a false identity, a thief could be hired into your organization and given access to critical systems and areas within your organization. Once trusted, this person could then arrange to steal cash and equipment, and disappear into the night. For this reason, background checks and a certain amount of due diligence work is necessary in order to verify that new hires are who they say they are. For more information on preventing identify theft, visit the Identity Theft Prevention Checklist at the following URL:

http://victimsassistanceofamerica.org/eduinfo/idtheft_prevention.cfm

## Identity Theft - What To Do If It Happens To You

1. Report it to the police
2. Cancel all credit cards
3. Call fraud units - Experian, Equifax, Trans Union
4. Notify banks
5. Fill out fraud affidavits to prove innocence
6. Get a new ATM card
7. Have SSN changed
8. Notify the passport authorities
9. Report stolen checks to TeleCheck, National Processing Company (NPC), and Equifax
10. Notify postal inspector if you suspect mail theft
11. Call telephone, electricity, and gas companies and alert them
12. Change drivers license number
13. Call Consumer Credit Counseling for help removing fraudulent claims from your record 800.388.2227
14. Keep a log of all conversations you have dealing with this, including names and dates
15. Consider seeking legal counsel.
16. Pay attention to your mental health
17. Change passwords everywhere
18. Change PIN numbers
19. Change e-mail addresses
20. Use common sense

## Recommendations for Preventing Identify Theft

**Prevent Identity Theft**

You can't guarantee that you will never be a victim, but you can minimize your risk with the following measures.

1. **Big Duh** - Don't give out personal information on the phone, through the mail or over the Internet *(through email or online forms, or any other manner)* unless you have initiated the contact or are sure you know who you're dealing with.

2. **Resist Providing Personal Information -** Before revealing any personally identifying information *(for example, on an application)*, find out how it will be used and secured, and whether it will be shared with others. Ask if you have a choice about the use of your information. Can you choose to have it kept confidential?

3. **Secure Your Home -** Secure personal information in your home in safes that are bolted to the floor, especially if you have roommates, employ outside help, or are having

service work done in your home. Securely store extra checks, credit cards, documents that list your Social Security number, and similar valuable items.

4. **Fool Burglars** - Don't advertise to burglars that you're away from home. Put lights on timers, temporarily stop delivery of your newspaper, and ask a neighbor to pick up any items that may arrive unexpectedly at your home.

5. **Guard Your Mail –** Pick up mail from your mailbox promptly. Do not send mail through your mailbox – a red flag raised on your mailbox is …well…a red flag for burglars that a check is probably waiting inside. If you're planning to be away from home and can't pick up your mail *(or are called away on an unexpected business trip or family emergency)*, call the U.S. Postal Service at 1-800-275-8777 to request a "vacation hold" or ask your carrier or a counter clerk for a "Authorization to Hold Mail" form *(PS Form 8076).* You might also consider purchasing and installing a relatively secure **"locking" mailbox** for either city or rural use.

6. **Guard Your Trash** - Protect your garbage. Identity thieves rummage through trash in your trash can or at landfills looking for personal information. To thwart identity thieves, who may pick through your trash or recycling bins to capture your personal information, tear or shred your...

    a. charge receipts,
    b. copies of credit applications,
    c. insurance forms,
    d. physician statements,
    e. checks and bank statements,
    f. credit card statements,
    g. expired charge cards that you're discarding,
    h. pre-approved credit card offers you get in the mail, and
    i. any documents that contain your social security number

7. **Opt-Out -** If you do not use the pre-screened credit card offers you receive in the mail, you can "opt out" by calling 1-888-5-OPTOUT *(1-888-567- 8688)*. You will be asked for your Social Security number in order for the credit bureaus to identify your file so that they can remove you from their lists and you still may receive some credit offers because some companies use different lists from the credit bureaus' lists.

   (If you do accept a credit card offer, be aware that some credit card companies, when sending out credit cards, have recently adopted security measures that allow a card recipient to activate the card only from his/her home phone number, but this is not yet a universal practice.)

8. **Purchase a Shredder –** Shredders come in a variety of styles and prices, starting with shredding scissors and exculpating to powerful shredders that can shred through binder clips.



9. **Limit, protect, and be aware of the type and amount of personal data you carry around...**

   Keep your purse/wallet and organizer/briefcase - as well as any copies you may retain of administrative forms that contain your sensitive personal information - in a safe place at work.

10. **Use PINS & Passwords -** Place passwords on your credit card, bank, brokerage and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Use a password instead.

11. **At Work -** Keep your purse or wallet in a safe place at work.


12. **Monitor Bills -** Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks. Check your bills/statements carefully and call companies if you do not receive regular bills in a timely manner. Make it your habit to review your bank and credit card statements as soon as you receive them and report any unauthorized transactions promptly so the accounts can be closed.

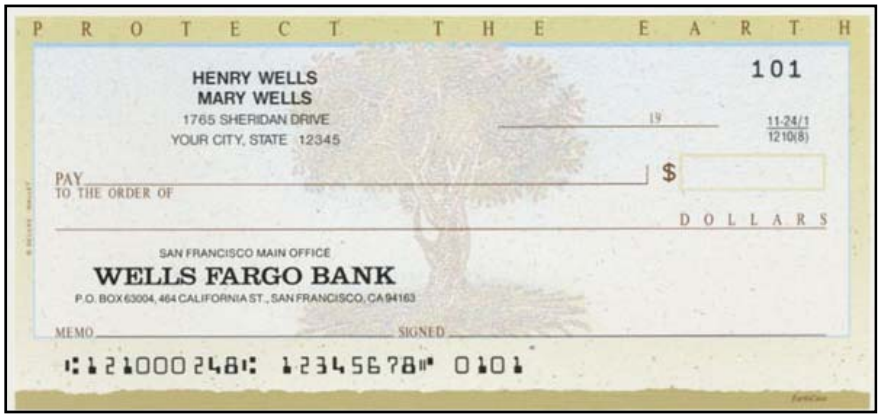
13. **Credit Card Photos -** Some issuers of bank and/or credit cards offer the option of adding the PHOTO of the named customer on the face of the card. If your issuer*(s)* offer this option, TAKE ADVANTAGE. It's certainly more difficult for someone else to use a card with your photo on it.


14. **Be Check Smart -** When ordering new checks, pick them up at the bank, rather than having them sent to your home mailbox. Consider using only your first initial(s) rather than your full name so a thief won't know what to sign. To save time, many people have their bank print every bit of personal info they can fit on personal checks to speed up check approval in the check-out line *(and minimize what they have to write-in by hand)*. Resist the urge. Don't put any information other than your name and address on your checks. Also, keep a close watch on your checkbook both when you're writing checks and when it is lying around.

    Some thieves use cleaning solvent to remove what is already written on a check, making it payable to themselves. To make this harder, you should write checks using a pen with thick, dark ink. Draw lines to fill in gaps in the spaces where you designate to whom a check is payable and the amount.

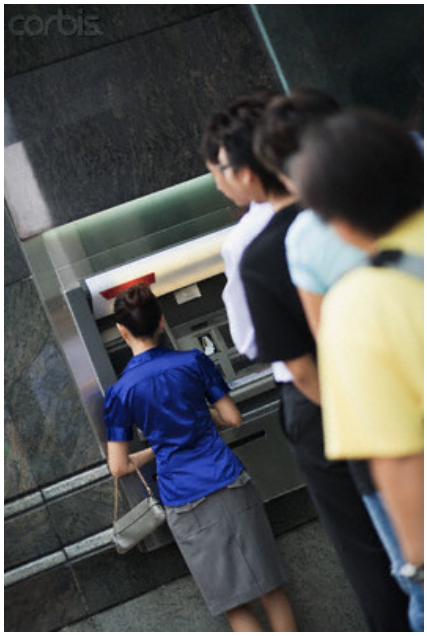
    If your checks have been stolen or misused, immediately notify your bank, place a stop payment order, and close your checking account. Also, immediately report to your bank

any irregularities in your bank statements. Report mail theft or tampering to the U.S. Postal Inspection Service, which is listed in your phone book




15. **GUARD deposit slips** as closely as you do checks. Not only do they have your name, address and account number printed on them, but they can also be used to withdraw money from your account. All a thief has to do is write a bad check, deposit it into your account and use the "less cash received" line to withdraw your money.

16. **Avoid Shoulder Surfers -** A "*shoulder-surfing*" identity thief can memorize your name, address and phone number during the short time it takes you to write a check. Also, in many public places "shoulder surfing" criminals can stand nearby and watch you punch in your phone-card number, debit-card PIN, credit card number, or even listen in on your conversation if you give your credit-card number over the phone for a hotel room or rental-car. Don't carry more checks that you need. Keep extra checks in a secure place.




17. **Bolster Your Insurance -** ID theft already is covered under some homeowners' policies; others will add it for as little as $25 a year. A stand-alone policy costs from $60 to $200.

18. **Be Careful in Job Searches -** Online recruiting business giants like Monster.com, CareerBuilder.com and HotJobs.com caution users about false online job listings that are sometimes posted by identity thieves to illegally collect personal information from unsuspecting job seekers.

19. **Check Your Credit Reports -** Order a copy of your credit report from each of the three major credit reporting agencies every year. Make sure it is accurate and includes only those activities you've authorized.

20. **Be Careful at Restaurants** - When paying at stores, restaurants, and other businesses, be methodical at the payment counter, ensuring you retrieve your driver's license or other ID, credit card and your credit slip copy after your purchase. Make sure that the person you give the credit card to really is the waiter or proper person.

21. **Xerox Your Wallet or Purse** – Take a few minutes to make paper copies of all of the cards and IDs you carry in your wallet or purse, including the backs as they contain contact phone numbers in the event of theft. Secure the copies in a safe pace.

22. **ATM Crime -** "Shoulder surfers" aren't limited to checkout stands and lines. Near ATMs, some sophisticated thieves will watch the victim use the card *(perhaps using high-powered binoculars, or even hidden cameras)* and learn the victim's personal identification number *(PIN)* and even the card number. Later, they'll steal the card or make their own and use ATMs to withdraw cash from your account. Watch for one or

more persons loitering around an ATM, often in a car, behind bushes or otherwise nearby. Use your body, or cup your other hand over the keypad, to "shield" it as you enter your PIN into the ATM. **Never** write your PIN on the back of your card; you could lose it, and some ATM scams involve a scammer "distracting" the victim and grabbing the card before running away.

23. **Drive up ATMs -** If you are using a drive-up ATM, keep your engine running and be sure your passenger windows are rolled up and all doors are locked. Before you roll down your window to use the ATM, observe the entire surrounding area; if anyone or anything appears to be suspicious, drive away at once. When possible, leave enough room between cars when you're in the ATM drive-up queue to allow for a quick exit, should it become necessary.

**24. Counterfeit Cashier's Check**

1. Inspect the cashier's check.
2. Ensure the amount of the check matches in figures and words.
3. Check to see that the account number is not shiny in appearance.
4. Be watchful that the drawer's signature is not traced.
5. Official checks are generally perforated on at least one side.
6. Inspect the check for additions, deletions, or other alterations.
7. Contact the financial institution on which the check was drawn to ensure legitimacy.
8. Obtain the bank's telephone number from a reliable source, not from the check itself.
9. Be cautious when dealing with individuals outside of your own country.

**25. Credit Card Fraud**

a. Ensure a site is secure and reputable before providing your credit card number online.
b. Don't trust a site just because it claims to be secure.
c. If purchasing merchandise, ensure it is from a reputable source.
d. Promptly reconcile credit card statements to avoid unauthorized charges.
e. Do your research to ensure legitimacy of the individual or company.
f. Beware of providing credit card information when requested through unsolicited emails.

**26. Debt Elimination**

a. Know who you are doing business with - do your research.
b. Obtain the name, address, and telephone number of the individual or company.
c. Research the individual or company to ensure they are authentic.
d. Contact the Better Business Bureau to determine the legitimacy of the company.
e. Be cautious when dealing with individuals outside of your own country.
f. Ensure you understand all terms and conditions of any agreement.
g. Be wary of businesses that operate from P.O. boxes or maildrops.

h. Ask for names of other customers of the individual or company and contact them.
i. If it sounds too good to be true, it probably is.

**27. DHL/UPS**

a. Beware of individuals using the DHL or UPS logo in any email communication.
b. Be suspicious when payment is requested by money transfer before the goods will be delivered.
c. Remember that DHL and UPS do not generally get involved in directly collecting payment from customers.
d. Fees associated with DHL or UPS transactions are only for shipping costs and never for other costs associated with online transactions.
e. Contact DHL or UPS to confirm the authenticity of email communications received.

**28. Employment/Business Opportunities**

a. Be wary of inflated claims of product effectiveness.
b. Be cautious of exaggerated claims of possible earnings or profits.
c. Beware when money is required up front for instructions or products.
d. Be leery when the job posting claims "no experience necessary".
e. Do not give your social security number when first interacting with your prospective employer.
f. Be cautious when dealing with individuals outside of your own country.
g. Be wary when replying to unsolicited emails for work-at-home employment.
h. Research the company to ensure they are authentic.
i. Contact the Better Business Bureau to determine the legitimacy of the company.

**29. Escrow Services Fraud**

a. Always type in the website address yourself rather than clicking on a link provided.
b. A legitimate website will be unique and will not duplicate the work of other companies.
c. Be cautious when a site requests payment to an "agent", instead of a corporate entity.
d. Be leery of escrow sites that only accept wire transfers or e-currency.
e. Be watchful of spelling errors, grammar problems, or inconsistent information.
f. Beware of sites that have escrow fees that are unreasonably low.

**30. Identity Theft**

a. Ensure websites are secure prior to submitting your credit card number.
b. Do your homework to ensure the business or website is legitimate.
c. Attempt to obtain a physical address, rather than a P.O. box or maildrop.
d. Never throw away credit card or bank statements in usable form.
e. Be aware of missed bills which could indicate your account has been taken over.

f. Be cautious of scams requiring you to provide your personal information.
g. Never give your credit card number over the phone unless you make the call.
h. Monitor your credit statements monthly for any fraudulent activity.
i. Report unauthorized transactions to your bank or credit card company as soon as possible.
j. Review a copy of your credit report at least once a year.

**31. Internet Extortion**

a. Security needs to be multi-layered so that numerous obstacles will be in the way of the intruder.
b. Ensure security is installed at every possible entry point.
c. Identify all machines connected to the Internet and assess the defense that's engaged.
d. Identify whether your servers are utilizing any ports that have been known to represent insecurities.
e. Ensure you are utilizing the most up-to-date patches for your software.

**32. Investment Fraud**

a. If the "opportunity" appears too good to be true, it probably is.
b. Beware of promises to make fast profits.
c. Do not invest in anything unless you understand the deal.
d. Don't assume a company is legitimate based on "appearance" of the website.
e. Be leery when responding to invesment offers received through unsolicited email.
f. Be wary of investments that offer high returns at little or no risk.
g. Independently verify the terms of any investment that you intend to make.
h. Research the parties involved and the nature of the investment.
i. Be cautious when dealing with individuals outside of your own country.
j. Contact the Better Business Bureau to determine the legitimacy of the company.

**33. Lotteries**

a. If the lottery winnings appear too good to be true, they probably are.
b. Be cautious when dealing with individuals outside of your own country.
c. Be leery if you do not remember entering a lottery or contest.
d. Be cautious if you receive a telephone call stating you are the winner in a lottery.
e. Beware of lotteries that charge a fee prior to delivery of your prize.
f. Be wary of demands to send additional money to be eligible for future winnings.
g. It is a violation of federal law to play a foreign lottery via mail or phone.

**34. Nigerian Letter or "419"**

a. If the "opportunity" appears too good to be true, it probably is.
b. Do not reply to emails asking for personal banking information.
c. Be wary of individuals representing themselves as foreign government officials.
d. Be cautious when dealing with individuals outside of your own country.

e. Beware when asked to assist in placing large sums of money in overseas bank accounts.
f. Do not believe the promise of large sums of money for your cooperation.
g. Guard your account information carefully.
h. Be cautious when additional fees are requested to further the transaction.

**35. Phishing/Spoofing**

a. Be suspicious of any unsolicited email requesting personal information.
b. Avoid filling out forms in email messages that ask for personal information.
c. Always compare the link in the email to the link that you are actually directed to.
d. Log on to the official website, instead of "linking" to it from an unsolicited email.
e. Contact the actual business that supposedly sent the email to verify if the email is genuine.

**36. Ponzi/Pyramid**

a. If the "opportunity" appears too good to be true, it probably is.
b. Beware of promises to make fast profits.
c. Exercise diligence in selecting investments.
d. Be vigilant in researching with whom you choose to invest.
e. Make sure you fully understand the investment prior to investing.
f. Be wary when you are required to bring in subsequent investors.
g. Independently verify the legitimacy of any investment.
h. Beware of references given by the promoter.

**37. Reshipping**

a. Be cautious if you are asked to ship packages to an "overseas home office."
b. Be cautious when dealing with individuals outside of your own country.
c. Be leery if the individual states that his country will not allow direct business shipments from the United States.
d. Be wary if the "ship to" address is yours but the name on the package is not.
e. Never provide your personal information to strangers in a chat room.
f. Don't accept packages that you didn't order.
g. If you receive packages that you didn't order, either refuse them upon delivery or contact the company where the package is from.

**38. Spam**

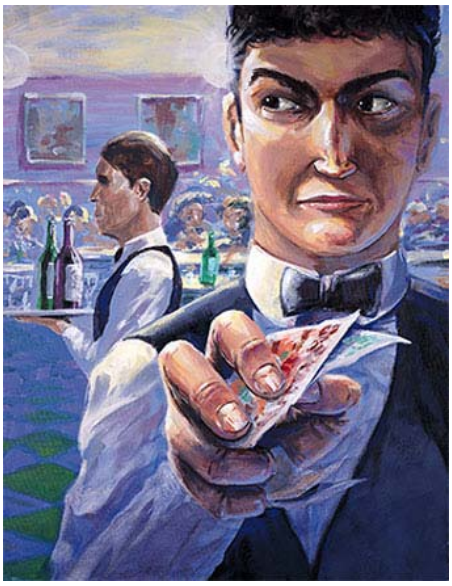
a. Don't open spam. Delete it unread.
b. Never respond to spam as this will confirm to the sender that it is a "live" email address.
c. Have a primary and secondary email address - one for people you know and one for all other purposes.
d. Avoid giving out your email address unless you know how it will be used.
e. Never purchase anything advertised through an unsolicited email.

**39. Third Party Receiver of Funds**

1. Do not agree to accept and wire payments for auctions that you did not post.
2. Be leery if the individual states that his country makes receiving these type of funds difficult.
3. Be cautious when the job posting claims "no experience necessary".
4. Be cautious when dealing with individuals outside of your own country.

## Chapter Review - Key Points

1. Identity theft has become rampant in recent years.
2. Detecting identity theft within a month helps significantly to minimize losses.
3. You should review/balance all of your statements each month.
4. 12% of all identity theft comes from discarded papers.
5. 11% of all identity theft comes from stolen wallets or purses.
6. 16% of all identity theft is committed by friends, relatives or co-workers.
7. It is easy for someone to masquerade as a legitimate employee or co-worker.
8. PINs can help minimize damage from identity theft.



# Employee Theft

## Chapter 27

## Employee Theft

The US Chamber of Commerce estimates that employee theft costs businesses $40 billion dollars each year. This total is ten times the value of street crime losses annually in the USA. Another study estimate employee theft and dishonesty costs U.S. businesses between $60 billion and $120 billion per year, not including the billions spent on protecting against theft. Presented below are a few statistics:

1. Employees out-steal shoplifters.

2. The US Chamber of Commerce estimates that 75% of all employees steal at least once, and that half of these steal again.

3. The Department of Justice reports cite lower numbers – estimating that nearly one-third of all employees commit some degree of employee theft.

4. Recent reports claim that employee theft is increasing at a rate of fifteen percent annually and according to the FBI, employee theft is one of the fastest growing crimes in the USA.

5. Some experts claim that one-third of all new businesses fail because of employee theft.

6. It is estimated that approximately two percent of all business sales are lost to employee theft.

7. The percentage of resumes and job applications that contain lies and exaggerations has been estimated between 30 and 80 percent. (Security Management Magazine)

8. 5% of professional hires have criminal records. (Source: HR Logic)

9. 75% of internal theft is undetected. ("How to Identify Dishonesty Within Your Business")

10. Employee theft amounts to 4% of food sales at a cost in excess of $8.5 billion annually. 75% of inventory shortages are attributed to employee theft. (National Restaurant Association)

11. The Labor Law Industry has increased by 2200%. (Equal Employment Opportunity Commission)

12. Employee theft costs between 1/2%-3% of a company's gross sales. Even if the figure is 1%, it still means employees steal over a billion dollars a week from their employers. ("How to Identify Dishonesty Within Your Business")

13. 30% of business failures are due to poor hiring practices. Annual losses generated by poor hires, absenteeism, drug abuse, and theft amount to $75 billion per year. (U.S. Department of Commerce-Atlanta Business Chronicle.)

## Employee Theft takes Many Forms

Employee theft can encompass many activities including:

1. Faking on-the-job injuries for compensation.
2. Taking merchandise.
3. Stealing small sums of cash.
4. Forging or destroying receipts.
5. Shipping and billing scams.
6. Putting fictitious employees on the payroll.
7. Falsifying expense records.

Employee theft may be a simple isolated event carried out by one individual, a highly organized scheme to acquire substantial financial or material gain, or anything in between.

## Preventing Employee Theft

Statistics indicate that only two percent of businesses that suffer losses from employee theft take subsequent steps to prevent future cases of employee theft.

To deal with the problem of employee theft, employers can:

1. **Better Hiring -** In general, establish a smart hiring process more likely to yield trustworthy employees (i.e. personal interviews, background checks, credit checks, etc.);

2. **Better Accounting -** In general, improve accounting practices and record keeping, establish an internal employee theft department, beef up security measures, and more.

3. **Pre-Screen Employees -** For as little as $10 you can check criminal records, credit history or other information. Background checks should include:

    a. Criminal history for crimes involving violence, theft, and fraud;
    b. Civil history for lawsuits involving collections, restraining orders, and fraud;
    c. Driver's license check for numerous or serious violations;
    d. Education verification for degrees from accredited institutions;
    e. Employment verification of positions, length of employment, and reasons for leaving.

4. **References -** Check and document references of each new hire.

5. **Conduct Frequent Physical Inventories -** Pilferage is one of the most common forms of internal loss. Reconcile sales to inventory on a quarterly basis, or at least annually, with the help of a third party. Conduct surprise inventories.

6. **Separate Bookkeeping Functions -** Misapplication of payments can lead to embezzlement. Do not let the same person who processes checks also manage the accounts receivable records.

7. **Personally Approve Bookkeeping Adjustments -** Approve any adjustments to the books no matter how slight – even adjustments to correct an error.

8. **Control Check Signers -** Limit the number of signatories to yourself and one or two highly trusted assistants. Keep blank checks under lock and key.

9. **Review Monthly Bank Statements -** Instruct your bank to send the monthly statement directly to you. Review the statement before passing it on to your bookkeeper. This review allows you to spot any improperly executed checks.

10. **Tighten Up On Petty Cash -** Allow only one or two trusted employees to disburse petty cash. Require that a receipt and a signed voucher be submitted for all petty cash disbursements.

11. **Separate Buying and Bookkeeping -** To maintain a system of checks and balances, assign ordering and payment responsibilities to different employees.

12. **Watch Company Credit Cards -** Require all credit cards be signed out and all credit card expenses be authorized by a purchase order.

13. **Document All Expense Reports -** Require strict documentation for all reimbursable expenses incurred by employees. Subject every expense account voucher to a pre-audit review procedure before payment.

14. **Have A Third Party Refund Policy -** Issue refunds only upon the approval of a third party, preferably a trusted assistant.

15. **Culture of Honesty** – Try to cultivate a culture of honesty within your organization. Short seminars, circulating articles, and recognizing and rewarding correct behavior. A positive work environment encourages employees to follow established policies and procedures, and act in the best interests of the organization. Fair employment practices, written job descriptions, clear organizational structure, comprehensive policies and procedures, open lines of communication between management and employees, and positive employee recognition will all help reduce the likelihood of internal fraud and theft.

16. **Security Cameras** – Install cameras throughout your facilities to record and capture all activities.

17. **Be Organized** – A well organized stock room, supply room or warehouse makes it easier to spot missing items.

18. **Test The System** – Remove some inventory, introduce a bogus invoice, etc - see how long it takes for your employees to discover the errors.

19. **Closing Procedures -** Prepare a check-list of closing and lock-up procedures for employees. Make sure appropriate employees understand what is expected.

20. **Security Tags -** Make sure all equipment is marked. Take time to mark company equipment with inventory tags or an electric pencil. Computers and computer-related equipment is vulnerable, particularly laptop computers. Use equipment serial numbers or a similar system to track equipment.

21. **Employee IDs -** Use an employee identification system, if practical. If you have many full- and part-time employees or you are having key management problems, an access system that requires the employee to insert an electronically coded card upon entering the business or specific areas will give additional control.

22. **Screen New Customers** – A common ploy occurs when employees sell goods to their friends, who in turn disappear and never pay. Take time to perform reasonable background checks on new customers to ensure their authenticity. Look up their address on Google maps, call the phone number to make sure it is valid, ask for letterhead and business cards, review the customer's web site, call and welcome the customer, visit the customer.

23. **Escalate Larger Accounting Transactions** – Implement measures to hold the processing of larger transactions until approved by a third party within your organization. The escalation threshold can be increased as employees earn more trust.

24. **Implement An Anonymous Reporting System** - Provide a confidential reporting system for employees, vendors, and customers to anonymously report any violations of policies and procedures.

25. **Perform Regular and Irregular Audits** – Perform regular and random unannounced financial audits and fraud assessments to help identify new vulnerabilities, and to measure the effectiveness of existing controls. This lets employees know that fraud prevention is a high priority for the organization.

26. **Investigate Every Incident -** A thorough and prompt investigation of policy and procedure violations, allegations of fraud, or warning signs of fraud will give you the facts you need to make informed decisions and reduce losses.

27. **Eliminate Temptations** – Eliminate as many temptations as you can by securing goods and cash, locking doors and drawers, and implementing well known controls.

28. **Keys** - Be careful with keys. Sign out all keys and collect them when employees leave the company. Better yet, move to electronic card keys that can be disabled when employees leave.

29. **Lead By Example -** Senior management and business owners set the example for the organization's employees. A cavalier attitude toward rules and regulations by management will soon be reflected in the attitude of employees. Every employee — regardless of position — should be held accountable for their actions.

30. **Use Consecutive Numbers -** Make sure all checks, purchase orders, and invoices are numbered consecutively, and regularly check for missing documents.

31. **For Deposit Only Stamp -** Use a "for deposit only" stamp on all incoming checks to prevent an employee from cashing them.

32. **Unopened Mail -** Unopened bank statements and canceled checks should be received by the business owner or outside accountant each month and they should carefully examine for any red-flag items such as missing check numbers. They should also look at the checks that have been issued to see if the payees are legitimate, and make sure that the signatures are not forgeries.

33. **Reconcile Statements** – The purpose of the bank statement reconciliation is to prove that the cash on the books agrees with the cash at the bank. It is difficult for an employee to hide theft when bank reconciliations are prepared monthly. Of course, bank reconciliations should be prepared by an outside person and need to be reviewed by management.

34. **Two Signatures -** Require all large checks to have two signatures. Never sign a blank check. Sign every payroll check personally. Avoid using a signature stamp.

35. **Insurance –** Consider obtaining an insurance policy that covers outside crime, employee theft and computer fraud. It will be there as a safety net in case your fraud prevention tactics don't work.

36. **Look for Stress -** Be alert to disgruntled or stressed employees, or those who have indicated that they are having financial difficulties. Also look for any unexplained significant rises in an employee's living standards.

# Employee Background Checks

## Chapter 28

## Employee Background Checks

With identity theft and cybercrime on the rise, and the ease in which Fake IDs and fake college diplomas can be obtained via the internet, it is more important than ever to conduct a background check on potential employees, if not all potential vendors and customers. There are dozens of background check companies to choose from charging fees ranging from $20 to $200 per background check. Some of the sources they commonly check are as follows:

1. **County Criminal Checks** - Search of superior, upper, lower, and/or municipal court records, across the country to determine if a subject has a felony or misdemeanor filing within the last seven years, or longer if the record includes a legally reportable conviction.

2. **National Criminal Database Search** - Search of aggregate databases of millions of records from various sources in the United States obtained by commercial vendors from the following sources:

    a. County Court Houses
    b. State Departments of Incarcerations
    c. State Record Repositories
    d. Probation Departments
    e. Townships
    f. Sex Offender Registries

3. **Social Security Number Traces –** A common mistake employers make is failing to cross-check the identity of their applicants with a Social Security Number Trace using credit history information. A proper background check should employ SSN Trace information to authenticate that the Social Security Number provided by your applicant is associated with an individual of the same name, that the approximate date of issue range of the SSN equates with your applicant's birth date, and that the address history associated with that SSN corresponds with the areas of the country where your applicant has lived, worked, attended school, or spent other significant time. This type of SSN Trace will usually turn up any alias names that have been associated with that SSN.

4. **Driver's License History Search** - This is an important search for applicants who are required to operate their vehicle for business purposes and/or driving a company vehicle. Records will show history over the past 3-7 years and are available in all 50 states and Washington DC. Reports will include all personal identifiers as well as offenses and citations.

5. **Pre-Employment Credit Reports -** Full credit report from one of the three nationwide credit bureaus. This report will offer insight into the applicant's reliability and a sense of their personal responsibility. This report will include derogatory credit information, public filings (bankruptcies, liens and judgments) as well as previous addresses. This can

be another great tool for identifying other counties that the applicant may have lived and is especially useful for companies whose candidates will have check-writing privileges or other access to company funds.

6. **Reference Interviews -** A verification of business and/or personal credentials is a valuable source of information about the applicant's general image as perceived by others. Results may offer insight into the candidate's trustworthiness, reliability, competency and integrity.

7. **Substance Abuse Screening -** Incorporating Substance Abuse Screening into your hiring process is now fairly easy. Most services offer Urine, Hair and Saliva testing at thousands of Patient Service Centers across the United States. Screens can be used for pre-employment, random and post-accident programs. Results are typically reviewed by board-certified Medical Review Officers (MRO), and handled in full compliance with federal DOT regulations and guidelines. Negative results are typically determined in 1-2 days.

8. **Homeland Security Check** - A Homeland Security Check is cross reference of your applicant’s name against over 45 worldwide databases of known terrorists, fugitives, individuals, organizations and companies considered to be a threat to global and national security. The Homeland Security Check database is updated daily as the various individual databases are modified.

9. **Education Verifications** - When hiring an individual, companies often base salary packages and positions on the individual's education. Failing to verify important information can result in appointing unqualified people to positions they don't deserve, which in turn affects your company's ability to compete. An Education Verification confirms schools attended, diplomas, degrees & certificates awarded, dates of attendance, and additional information as available.

10. **Employment Verifications** - Some candidates may be less than truthful about their employment history. Research shows this to be the number one discrepancy on resumes and job applications. A proper background check should verify information on your applicant's resume. Dates of employment, starting and ending positions and salaries, reason for termination, and eligibility for re-hire are examples of the information employers should be asked to verify. If possible, the background check should include an interview of the candidate’s supervisor to gain more personal knowledge of the applicant's skills and functionality in the workplace.

11. **Federal Criminal Court Searches** - There are many crimes that don't necessarily fall under local laws, they fall under federal jurisdiction. These crimes may include: tax evasion, embezzlement, counterfeiting, bank robbery and many other "white collar" crimes. This search lists criminal filings in any of the nation's federal district courts.

12. **Sex Offender Registry** - A Sex Offender Registry Search should be conducted to see if your subject is a registered offender.

13. **Global Screening Services** – Some background checks include searches on applicants that have lived or reside outside of the US. Many services are able to execute a Criminal Records Search in over 150 countries and Employment and Education Verifications in over 200 countries throughout the world.

14. **Workers Compensation** - A check of the state(s) worker's compensation commissions in the area(s) where the candidate has resided, to locate any claim history. The investigation is conducted in compliance with the Americans For Disabilities Act (ADA).

15. **Electronic Employment Eligibility Process (I-9)** - This process typically includes a "smart" error-detecting I-9 form, electronic archival of completed forms and instant confirmation of Employment Eligibility Status. This program is in compliance with the government's E-Verify program.

16. **Professional Licenses & Certifications** - Includes a review and verification of professional license and registration status of any license or certification required by industry or organizational standards. We verify all licenses and certifications provided by the candidate directly with the issuing or accrediting organization.

17. **Neighbor Checks** – Some background checks include locating and interviewing neighbors who have lived next to or near the applicant.

18. **Military Records Verification** – Military records can be searched to confirm military service, including dates of service and ranks reached.

## Background Check Privacy

There are some questions that cannot be asked, and information that cannot be relied upon when hiring an employee. In general, these questions revolve around disabilities, bankruptcy, criminal convictions after a certain number of years, and medical records. Depending upon the state where you operate, these topics and others may be off limits. To protect yourself, you should make yourself familiar with the laws in your state, and you should obtain written permission from the applicant to conduct a background check.

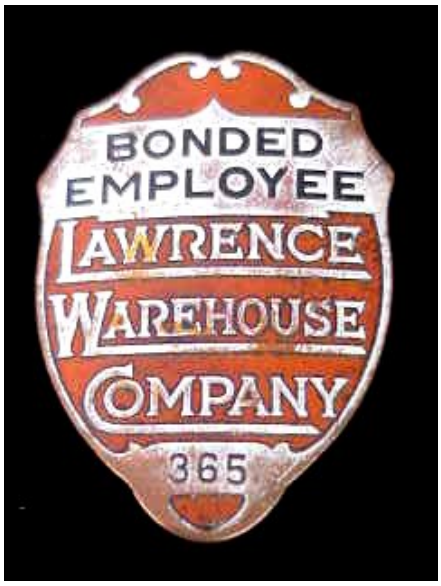
Some employers say that asking for written permission from the applicant to conduct a background check often is all that is needed for some applicants to admit to additional history that may be pertinent to the hiring decision.

## Letters of Reference

You should always require letters of reference, and these letters of reference should be investigated to make sure that they are authentic before making the final hire decision.

## Background Checking Services

1. www.trudiligence.com - Many searches with instant results. Free 1 week Trial.
2. www.formi9.com - Electronic I-9s. Expert I-9 Audits. Instant Employment Eligibility Verification.
3. find.intelius.com - $29.95 - Instant Criminal & Background Check, SSN Verification, Sexual offender registry, and Address trace in one! FCRA compliant.
4. www.Intelius.com - Instant Criminal & Background Check SSN Verification/FCRA (877)974-1500
5. www.CriteriaCorp.com - Screen Employees with Personality, Aptitude, Skills Tests.
   www.HireRight.com - Industry's fastest turnaround time. Trusted by Fortune 500.
6. www.infolinkscreening.com - Accurate and compliant employee background checks, drug testing, physical exams, and Form I-9 eSolutions provided by Kroll.
7. www.sentrylink.com - Instant online results for criminal checks, driving records, and credit reports. FCRA compliant. National criminal check only $19.95.
8. www.IntegraScan.com/Employee-Screening - $18.95 - Free preliminary results. Instantly check millions of records - $18.95. Comprehensive state and national background checks.
9. www.backgroundsonline.com - Professional employment background screening, hire with confidence!
10. www.CorporateScreening.com - Medical, Manufacturing, Financial Quality Customized Services
11. www.absolutebackgrounds.com - Provider of online applicant-screening services.
12. www.backgroundcheckgateway.com - Site enables visitors to perform free background checks, using public records.
13. www.backgroundchecks.com - A service which provides instant desktop delivery of criminal records information, social security validation and more.
14. www.backgroundsonline.com - Provider of web-based pre-employment screening services and employee background checks, including criminal, reference, DMV, education and employment verification.
15. www.brainbench.com - Provider of Internet-based applicant testing services, including technical, language and programmer/analyst aptitude testing.
16. www.corporate-screening.com - Provides national employee and business background online.
17. www.esrcheck.com - Firm offers pre-employment screening services for employers, human resources and security departments.
18. www.hireright.com - Provider of online pre-employment screening services.
19. www.informus.com - Provides internet-based employee screening.
20. www.sentrylink.com - Instant online results for criminal checks, driving records, and credit reports. FCRA compliant. National criminal check only $19.95.
21. www.trudiligence.com - Many searches with instant results. Compare vendors. Free 1 week Trial.
22. www.peoplewise.com - Provider of legally compliant, employment screening services over the Internet.
23. www.prsinet.com - Provider of pre-employment screening through background checks. Provides a web based order and retrieval system.
24. www.reviewnet.net - Provider of Internet-based solutions to attract, screen, interview and retain technology professionals.
25. www.NetDetective.com




# Bonding Employees

## Chapter 29

## Bonding Employees

Bonding is "an insurance contract in which an agency guarantees payment to an employer in the event of unforeseen financial loss through the actions of an employee."

In a perfect world, employee theft would never happen. Unfortunately, it does. To protect yourself, bonding helps assure that employees are trustworthy. And, if something should go amiss, it will be replaced. How important is bonding? One report claims that one-third of all bankruptcies are caused by employee theft, *(according to Marc Leclair, Assistant Vice President of Corporate Risk with London Guarantee).*

## When to Bond Your Employees

In general, you should consider bonding employees whenever they have access to expensive inventory or large sums of cash. "Statistically speaking, you may be surprised to learn that the employees most likely to steal from you are the longstanding employees who have been with you for 10 to 15 years. The employees that have been at the same position for years understand the accounting system to the point where they can actually play games with the numbers without you seeing the changes. Bank employees and warehouse workers are examples of employees that are typically bonded.

## Why You Bond Employees

Employees who have been convicted of fraud in the past are not usually able to get coverage, so bonding helps avoid the wrong employees to start with. Employers also use fidelity bonds to protect themselves from theft. There are four basic types of fidelity bonds, as follows:

1. ***individual*** *- Covers one employee (usually purchased by small concerns or family-operated businesses with only one employee)*

2. ***Name Schedule Fidelity Bond*** - You designate a set amount of coverage for a list of employees that you provide for the insurance company. Each time you hire a new employee, you have to contact the insurance company to have that person added to the list, if you choose to do so. Collection under this coverage hinges on absolute proof that an employee did in fact steal from you.

3. ***Blanket Position Bond*** - Under this type of bond, you specify coverage for a position rather than the individual. Each employee of a business is covered, and new employees are added automatically. Coverage is offered for each employee up to the maximum set out in the insurance policy. Blanket position bonds don't require proof of the individual responsible for the theft.

4. ***Primary Commercial Blanket Bond*** - Like the Blanket Position Bond, this bond covers each employee in the company. This type of coverage does not accommodate each employee, but rather treats the employees as one unit. In other words, it does not

matter if one or five people were involved in the crime, you will be able to claim the same amount.

## The Federal Bonding Program / Fidelity Bonding

A federal fidelity bond is NO COST insurance coverage meant to allow employers to hire job applicants considered "at risk" due to their past life experiences, protecting employers against employee dishonesty, theft or embezzlement. Since the program's inception in 1966, approximately 43,000 bonds have been issued with a 99% success rate. And, users have the added benefit of turning unemployed applicants into tax paying workers! Federal bonding may be provided to any individual who:

1. may have a dishonorable military discharge,
2. may have a record of arrest, conviction or imprisonment,
3. lacks work history,
4. has a poor credit history, and
5. has an offer of full-time employment

Note: Self employed individuals are not eligible

The process is simple and quick. Employers are not required to fill out forms. Employers, on behalf of the job applicant can request Fidelity Bonding by contacting the appropriate local department in person or via telephone. If an applicant and job meet eligibility criteria, bonding become effective immediately following certification and on the applicant's first day of work. Upon certification, the coverage provider mails the bond directly to the employer.

**Coverage -** An employee can be bonded for at least $5,000. The bond initially covers a six-month period beginning the first day of employment. After that time, if a bond still remains a condition of employment, employers can request a renewal for an additional six months (only one renewal per bond issued) or purchase the bond through the contracted insurance company at current commercial rates.

Additional information on the Fidelity Bonding is available at your local Employment and Training Center in your state. Bonding coordinators are available to help employers match the amount of bond coverage to the requirements of the position. Employers may also contact the State Bonding Coordinator at 312/793-9741.

## Key Points

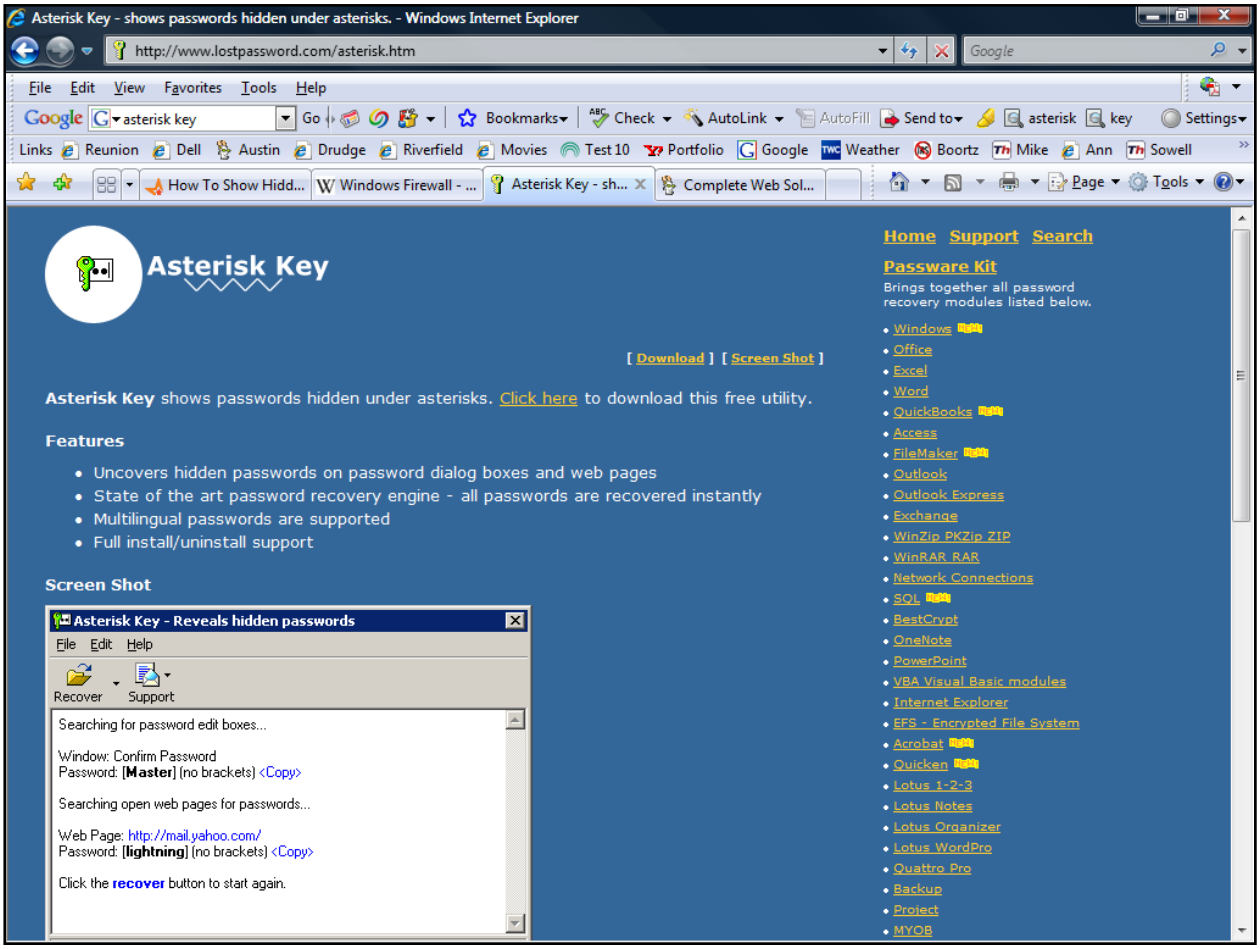
1. Bonding is simply a form of insurance protecting you from employee theft.
2. Bonding is recommended when employees have access to expensive inventory or large sums of cash.
3. Long standing employees (15 to 20 years) are more likely to steal.
4. There are four types of bonds.
5. Federal bonding is sometimes available for free.


# Asterisk Key

# Chapter 30

## Asterisk Key

This is a free utility that you can download (http://www.lostpassword.com/asterisk.htm) to reveal the passwords hidden under asterisks. It can instantly reveal any hidden password that is saved in a password dialog box or web page.




Of course you need access to the computer, and the computer must have the password remembered in order for this to work. Still, the existence of tools like this shows the vulnerability that occurs when you save your passwords on your computer.


# Encryption Analyzer & Passware Kit

## Chapter 31

# Encryption Analyzer

Encryption Analyzer is a free downloadable utility program that locates all of the password-protected or encrypted files on a PC or on PCs across a network. Key features are as follows:

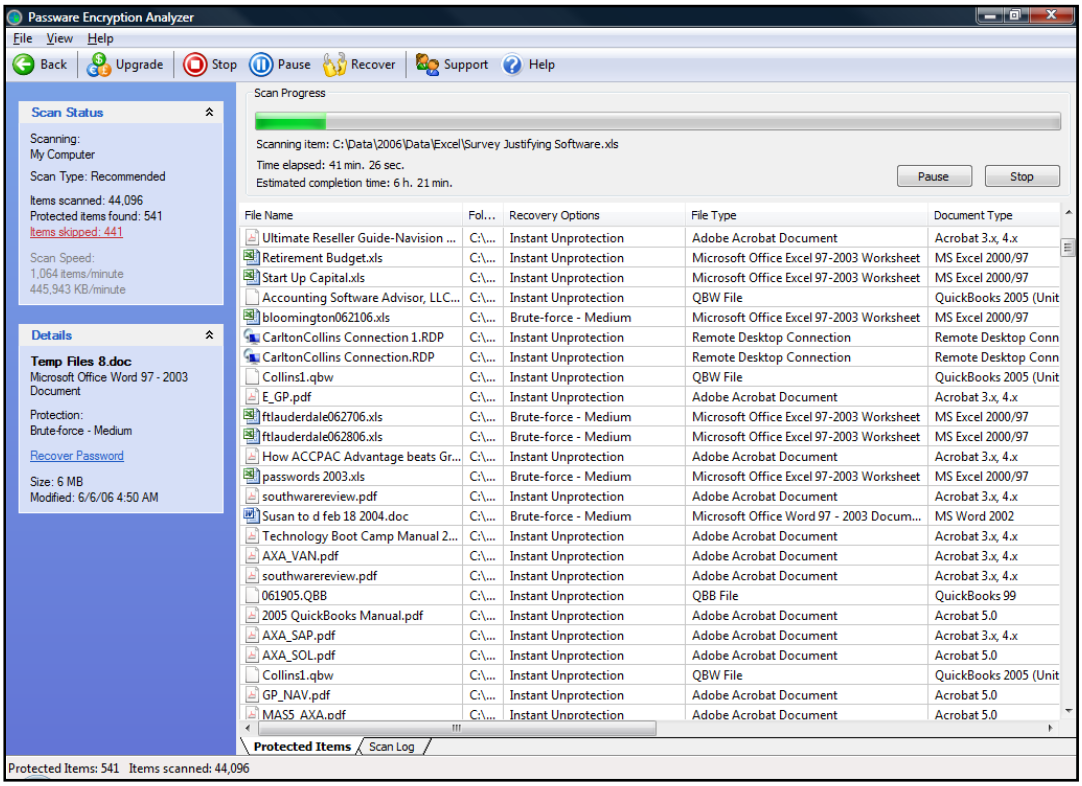
1. Scans files fast - over 4,000 files per minute on an average PC.

2. Supports over 100 different file formats.

3. Lists recovery options and launches appropriate password recovery modules if necessary. Provides detailed information: file formats, protection methods.

Legitimately, you can use this product to verify that you have applied passwords to your important files. IT Professionals can also use the product to ensure that users are applying proper password protection. Legitimately, Encryption Analyzer solves the common problem when employees leave a company without providing a complete list of their passwords.

I used Encryption Analyzer on my computer and found 541 protected files in 41 minutes, as shown in the screen below. Once identified, the files can then be opened using the affiliated Passware kit discussed on the following page.



## Passware Kit

Passware Kit is priced starting at $195. The product includes over 25 password recovery modules. Passware kit claims to crack the following files:

| | |
|---|---|
| 1. Windows | 2. Office |
| 3. Excel | 4. Word |
| 5. QuickBooks | 6. Access |
| 7. FileMaker | 8. Outlook |
| 9. Outlook Express | 10. Exchange |
| 11. WinZip PKZip ZIP | 12. WinRAR RAR |
| 13. Network Connections | 14. SQL |
| 15. BestCrypt | 16. OneNote |
| 17. PowerPoint | 18. VBA Visual Basic modules |
| 19. Internet Explorer | 20. EFS - Encrypted File System |
| 21. Acrobat | 22. Quicken |
| 23. Lotus 1-2-3 | 24. Lotus Notes |
| 25. Lotus Organizer | 26. Lotus WordPro |
| 27. Quattro Pro | 28. QuickBooks 2008 |
| 29. Quicken 2008 | 30. Quicken databases up to 2007 |
| 31. Backup | 32. Project |
| 33. MYOB | 34. Peachtree |
| 35. Paradox | 36. ACT! |
| 37. Mail | 38. Schedule+ |
| 39. Money | 40. WordPerfect |

# Securing Desktop Computers

## Chapter 32

## Desktop Computer Theft

While laptop computers are most often stolen, desktop computers tend to be left unattended in empty buildings. This fact gives rise to special considerations for securing desktop machines. Specifically, desktop computers should be locked up and bolted down as to deter or prevent theft. Presented below are anti-theft devices that may help you prevent the theft of your desktop computers.

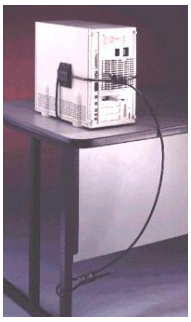
## Anti-Theft Products

**Desktop Locking Devices**

**Security Guard**

**Biometric Security Device**

**Bolt on Anti-Theft Cable Systems**



**Locking Anti-Theft Cable Systems**

**Retinal Scanners to gain access to Offices**

**Locking Cables**

**UV Marking Kits**

**Fake Security Camera**

**Security Camera Systems**

**Hidden Camera**

**See Thru Mirrors**

**Mirrored Ceiling Domes**

**Dead Bolts**

**Outdoor Security Lighting**

## Computer Protection Measures

There are several measures you can take to better secure your offices and computer systems. For example, you could make sure that your building is very secure to prevent intruders and theft. Install extra window locks and door locks. Consider hiring a building guard. Install key entry systems that monitor and record employee access. Install door locks on internal doors to prevent access to file servers & systems. Use computer locks to bolt computers to desks and tables. Use computer locks to protect laptop computers when traveling.

## Power Failure

Power failures represent the most frequent cause of data loss, which is a sad fact to report considering how easy this problem is to avoid. All computer systems should be equipped with an uninterruptible power supply (UPS) device to protect from power outages and power surges. For example, American Power Corporation produces a wide variety of UPS devices and surge suppressors.

APC offers more than 150 of these devices ranging in price from $40 to more than $80,000. Most businesses' computers can be protected from power failure for about $60 to $250,

depending upon the amount of battery time you prefer. All APC UPS products include PowerChute software that can be set to close your applications and shut down your computer automatically and gracefully in the event of a prolonged power failure in your absence. Another benefit of using an APC device is the automatic insurance which covers any electrical-related damage to your computer up to $25,000. These UPS devices can also protect your phone systems and television cable hook ups as well.

You should use a UPS device to protect your entire computer system including monitors, hubs, routers, and externally connected devices. The one exception to this rule is printers because they are typically a big drain on power. Therefore, unless you have a powerful UPS device, you should avoid plugging your printer into your UPS, but be sure to always use a surge protector.

## Computer Failure

Computer components can fail. The most common computer failures can be attributed to power supplies, hard drives, and system mother boards. However other components such as ram chips, processors, circuit boards, floppy disk drives, CD drives, and monitors can go bad as well. Today, most newer computers can be repaired quickly by replacing the damaged item; however legacy computers may take time to repair as replacement parts are often only available on the used market. Do not attempt to operate a visibly damaged computer. If your computer is making an unusual noise, turn it off. There is a good chance that a noisy computer has suffered or will suffer a head crash, hence the faster it is deactivated, the better the chance for data recovery.

If your computer does fail, do not automatically turn to recovery software. If you suspect that you may have lost access to data due to electrical or mechanical failure, software can't help. Using file recovery utilities on a faulty hard drive can destroy what was recoverable data. When a drive failure is suspected, turn off the machine. Call in a computer systems recovery specialist with the proper training and experience. Lost data can become unrecoverable data when un- or under-qualified personnel misuse file recovery utilities, open disk drives, and lack the basic skills necessary to properly maintain and repair computer equipment and data.

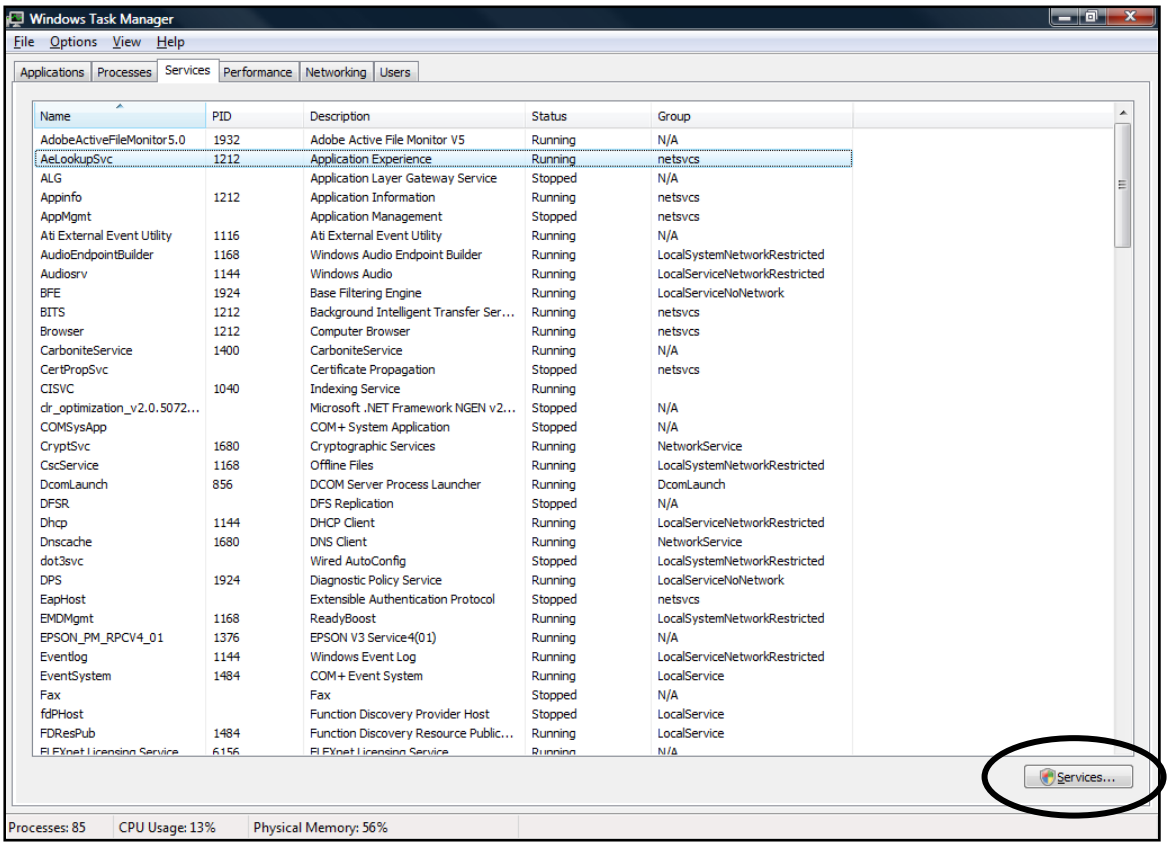
# Windows Security

## Windows Services

## Chapter 33

## Windows Services

Widows Services are Windows components (or programs) that run in the background of Windows to perform specific functions. They generally start each time the Microsoft Windows operating system is booted and continue running in the background as long as Windows is running. They appear in the processes list in Windows Task Manager as shown below:



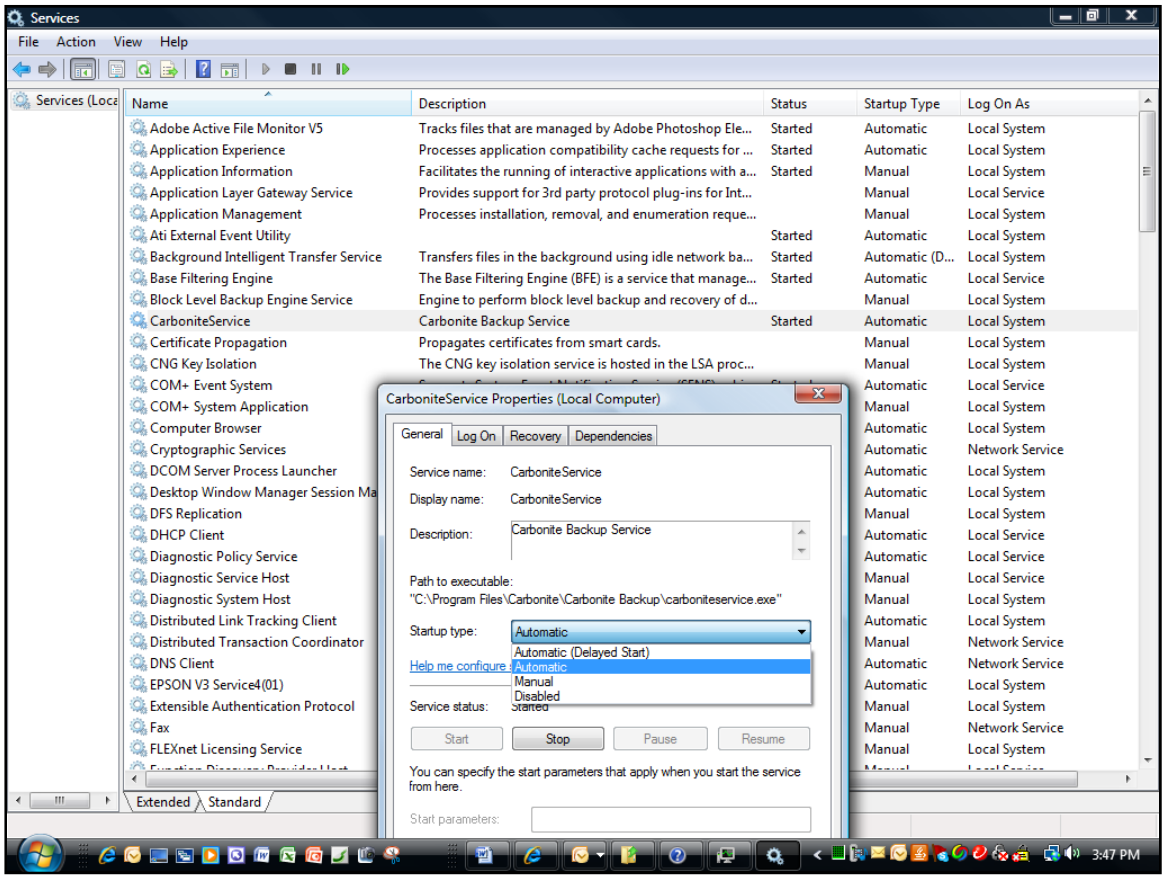

As a general rule you should turn off all Windows Services that you do not need, and check to make sure that rouge applets are not running as a Windows Services. As a result of clearing your Windows Services, your computer will perform faster, and there will be fewer services which might give a hacker tunnel access to your computer system. To turn off a service, select "Services" from the Windows Control Panel as circled above or run "Services.msc" using the “Run Command” on the “Start Menu”.

As an example, in the screen below I have entered Windows Services Administration Tool and right clicked on the Carbonite Service. Here I can accomplish the following:

1. Start, stop, pause or restart services.
2. Specify service parameters.
3. Change the startup type which includes Automatic, Manual and Disabled:
    a. Automatic starts the services at system logon.

b. Manual starts a service as required or when called from an application.
c. Disabled completely disables the service.
d. Automatic (Delayed) is a new startup type introduced in Windows Vista, that starts the service a short while after the system has finished booting and initial busy operations, so that the system boots up faster.

4. Change the account under which the service logs on.
5. Configure recovery options upon service failure.
6. Export the list of services as a text file or a CSV file.




Repeat this step to disable any unused services. The services you use may be different from the ones my computer uses; therefore, it is difficult to advise you as to exactly which services you should disable. Listed below are the most commonly unused services, but read through the remaining services in your Computer Management window to identify any other services you may not be using.

**Windows Vista Services that Most Users Should Consider Disabling**
**(55 Out of 154 Services Should Be Disabled)**

1. Application Experience
2. Application Layer Gateway Service
3. Application Management

4. Certificate Propagation
5. DFS Replication
6. Diagnostic Policy Service
7. Diagnostic Service Host
8. Diagnostic System Host
9. Distributed Link Tracking Client
10. Distributed Transaction Coordinator
11. Fax
12. Function Discovery Provider Host
13. Function Discovery Resource Publication
14. Health Key and Certificate Management
15. Human Interface Device Access
16. IKE and AuthIP IPsec Keying Modules
17. Interactive Services Detection **
18. Internet Connection Sharing (ICS)
19. IP Helper
20. IPsec Policy Agent
21. KtmRm for Distributed Transaction Coordinator
22. Link-Layer Topology Discovery Mapper
23. Microsoft iSCSI Initiator Service
24. Netlogon
25. Network Access Protection Agent
26. Offline Files
27. Parental Controls
28. Peer Name Resolution Protocol
29. Peer Networking Grouping
30. Peer Networking Identity Manager
31. PnP-X IP Bus Enumerator
32. PNRP Machine Name Publication Service
33. Portable Device Enumerator Service
34. Problem Reports and Solutions Control Panel Support
35. Quality Windows Audio Video Experience
36. Remote Registry
37. Secure Socket Tunneling Protocol Service **
38. Smart Card
39. Smart Card Removal Policy
40. SNMP Trap
41. Tablet PC Input Service
42. Terminal Services UserMode Port Redirector
43. Virtual Disk
44. WebClient
45. Windows CardSpace
46. Windows Connect Now - Config Registrar
47. Windows Error Reporting Service

48. Windows Image Acquisition (WIA)
49. Windows Media Center Receiver Service
50. Windows Media Center Scheduler Service
51. Windows Media Center Service Launcher
52. Windows Media Player Network Sharing Service
53. Windows Remote Management (WS-Management)
54. Windows Search
55. WinHTTP Web Proxy Auto-Discovery Service

**Comments about Adjusting your Windows Services**

2. Before adjusting your service settings, first install all Windows Updates.
3. If you are unsure whether you need a specific service or not, read the Description field.
4. If you are still in doubt, my recommendation is to leave the default setting.
5. Service settings are global, meaning changes apply to all users.
6. If you still unsure? Put your setting to "Manual" or the listing under "Safe." Manual allows Windows Vista to start the service when it needs to but not at boot up.
7. If you need a service, make it Automatic.
8. After adjusting your service settings, reboot your computer.

For a better source of information on Windows Services, visit http://www.blackviper.com/. This web site provides a current list of Windows services that should be disabled for each version of Windows, and provides your choice of “Safe”, “Tweaked” and “Bare Bones” recommendations. Shown below is a small sample of this web site’s tables.

**Black Viper's Windows Vista SP1 Service Configurations**
**(Sample Only)**

| Display Name | DEFAULT Home Basic | DEFAULT Home Premium | DEFAULT Business | DEFAULT Ultimate | "Safe" | "Tweaked" | "Bare Bones" |
|---|---|---|---|---|---|---|---|
| Application Experience | Automatic (Started) | Automatic (Started) | Automatic (Started) | Automatic (Started) | Automatic | Disabled * | Disabled * |
| Application Information | Manual (Started) | Manual (Started) | Manual (Started) | Manual (Started) | Manual | Manual | Manual |
| Application Layer Gateway Service | Manual | Manual | Manual | Manual | Manual | Disabled * | Disabled * |
| Application Management | Not Available | Not Available | Manual | Manual | Manual | Disabled * | Disabled * |

Similar services are offered at www.LabMice.net and www.TheElderGeek.com.

# Risk of Fire

## Chapter 34

## Risk of Fire

All of the passwords and security settings in the world won't help much in the event that your facility burns down. Therefore in a discussion about security, it is prudent to discuss the threat of fire and provide possible measures for minimizing that threat.

As a service, your local Fire Marshall will usually visit your facility for free and inspect your building in order to identify potential fire threats and provide you with suggestions for minimizing the risk of fire. Presented below is a sensible checklist that you should use to help you identify any obvious measures you can take to minimize the risk of fire. If you answer "No" to any of these items, then perhaps you should take measures to better secure your facilities.

## Fire Prevention Checklist

1. *Is the address of your property clearly visible and marked in large numbers that can be easily seen from the street?*
2. *Are fire proof filing cabinets adequately used to protect printed information?*
3. *Are computers elevated off the floor in order to prevent damage from water in the event that sprinklers or fire hoses are used to put out a fire?*
4. *Are there adequate smoke detectors in the building?*
5. *Are smoke detectors operational?*
6. *Are smoke alarm batteries changed at regular intervals? (twice a year)*
7. *Are smoke alarms tested regularly (twice a year)?*
8. *Are evaluation signs properly posted?*
9. *Are exit signs properly displayed?*
10. *Are all exits accessible with using a key? (ie: not dead bolted)*
11. *Do you have emergency lighting and does it work?*
12. *Do you have at least two plans of escape?*
13. *Does the plan call for a safe meeting place outside the building so employees can be quickly accounted for?*
14. *Are plans of escaped practiced regularly?*
15. *Are there adequate fire extinguishers in the building?*
16. *Are the areas outside and around the building free of weeds, debris and trash?*
17. *Is the use of all extension cords and power strips inspected for proper use?*
18. *Are extinguishers in place, serviceable and clear of obstruction?*
19. *Are extinguisher tags current?*
20. *Are there adequate sprinklers used throughout the building?*
21. *Is there .5 meter clear space below all sprinklers heads?*
22. *Are there fire hoses in the building?*
23. *Are those fire hoses in cabinet properly racked and in good condition?*
24. *Is there a fire water storage tank in the building?*
25. *Is the fire water storage tank to proper level?*
26. *Is the electrical room secured?*

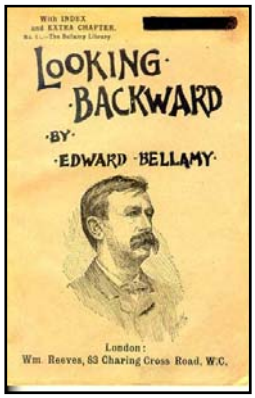
27. *Is the electrical room clear of combustible material?*
28. *Is there 3 feet of clear space around all electrical panels?*
29. *Is the mechanical room secured?*
30. *Is the mechanical room combustion air intake clear?*
31. *Is the mechanical room clear of combustible material?*
32. *Are there any fuel spills/leaks in the mechanical room?*
33. *Are there any fuel spills/leaks in the generator room?*
34. *Are attic fire separations intact?*
35. *Is the attic clear of combustible material?*
36. *Is the attic access secured?*
37. *Are crawl space fire separators intact?*
38. *Is the crawl space clear of combustible material?*
39. *Is the crawl space access secured?*
40. *Are the storage areas secured?*
41. *Are the custodial rooms secured?*
42. *Are emergency lights operational?*
43. *Is flammable material properly stored?*
44. *Is any gas-powered equipment stored in the building?*
45. *If smoking is allowed, are there adequate fire proof receptacles available in all smoking venues?*
46. *If smoking is not allowed, are no smoking signs displayed and are non-smoking rules enforced?*
47. *Are all electrical cover plates in place?*
48. *Are kitchen exhaust fans operational and clean?*
49. *Is kitchen fire suppression system maintained to schedule?*
50. *Is kitchen fire suppression system charged?*
51. *Are tree branches properly trimmed annually near electrical power lines?*
52. *Have the proper fire resistant materials been used where possible in the construction of the building?*
53. *Are all exterior vents, attics and eaves covered with mesh to prevent rodents from nesting or chewing through wires?*
54. *Do you know your local emergency number for fire-police-ambulance, and do you have it posted near you phones?*
55. *Are furnaces, stoves, and flue pipes properly maintained and inspected?*
56. *Are portable space heaters properly maintained and used only in compliance with company policy?*
57. *Is the central heating system inspected annually by a qualified technician?*
58. *Have you catalogued and updated your inventory list for insurance claims?*


# Credit Card Fraud

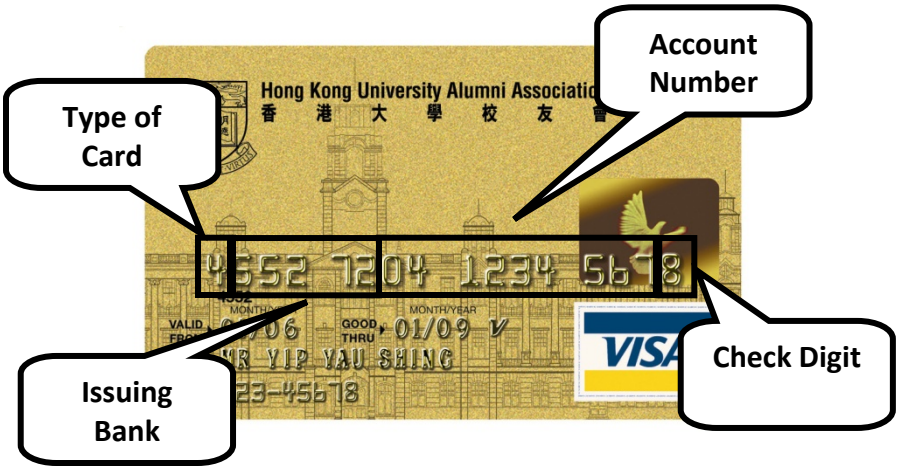
## Chapter 35

The strategy for generating credit card numbers is widely known, and the materials and equipment for producing fraudulent credit cards is also available. Hopefully, this information will make you more savvy when it comes to inspecting and accepting credit cards in your business.

The concept of using a card for purchases was described in 1887 by Edward Bellamy in his utopian novel *Looking Backward*. Bellamy used the term *credit card* eleven times in this novel.




**How Valid Credit Card Numbers Are Generated -** Presented below is a brief explanation of what the numbers on a typical credit card number mean.



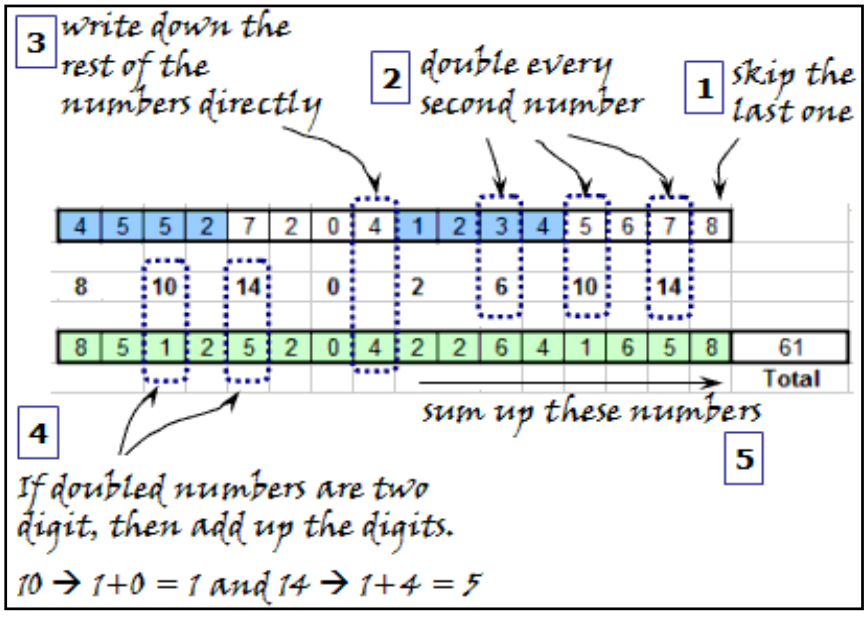

1. There are 16 numbers on a typical credit card.
2. The first number indicates which type of card the number belongs to. 3 = American Express or Diners Club, 4 = VISA, 5 = MasterCard, and 6 = DiscoverCard.
3. The next 5 digits identify the bank, or the issuer.
4. The next 9 digits form the "account number". (These nine number positions can be used to create 1 billion possible account numbers.)
5. The last digit is known as the "check digit" which is generated to satisfy a certain condition known as the Luhn check.

6. With each account number, there is always an unique check digit associated (for a given issuer identifier and an account number, there cannot be more than one correct check digit)
7. American Express issues credit cards with15 digits. The account numbers in this case are 8 digits long.

**The "Luhn" Check Digit -** In 1954, Hans Luhn of IBM proposed an algorithm to be used as a validity criterion for a given set of numbers. Almost all credit card numbers are generated following this validity criterion…also called as the Luhn check or the Mod 10 check. Today, the Luhn check is also used to verify a given existing card number. If a credit card number does not satisfy this check, it is not a valid number. For a 16 digit credit card number, the Luhn check can be described as follows:

1. Working right to left (starting with the check digit), double the value of every second digit. For example, in a 16 digit credit card number, double the 15th, 13th, 11th, 9th…digits (digits in odd places). In all, you will need to double eight digits.
2. If doubling of a number results in a two digit number, add up the digits to get a single digit number. This will result in eight single digit numbers.
3. Now, replace the digits in the odd places (in the original credit card number) with these new single digit numbers to get a new 16 digit number.
4. Add up all the digits in this new number. If the final total is perfectly divisible by 10, then the credit card number is valid (Luhn check is satisfied), else it is invalid.

**Example –** The credit card number used above is invalid. Let's apply the Luhn algorithm to this card to find out why.

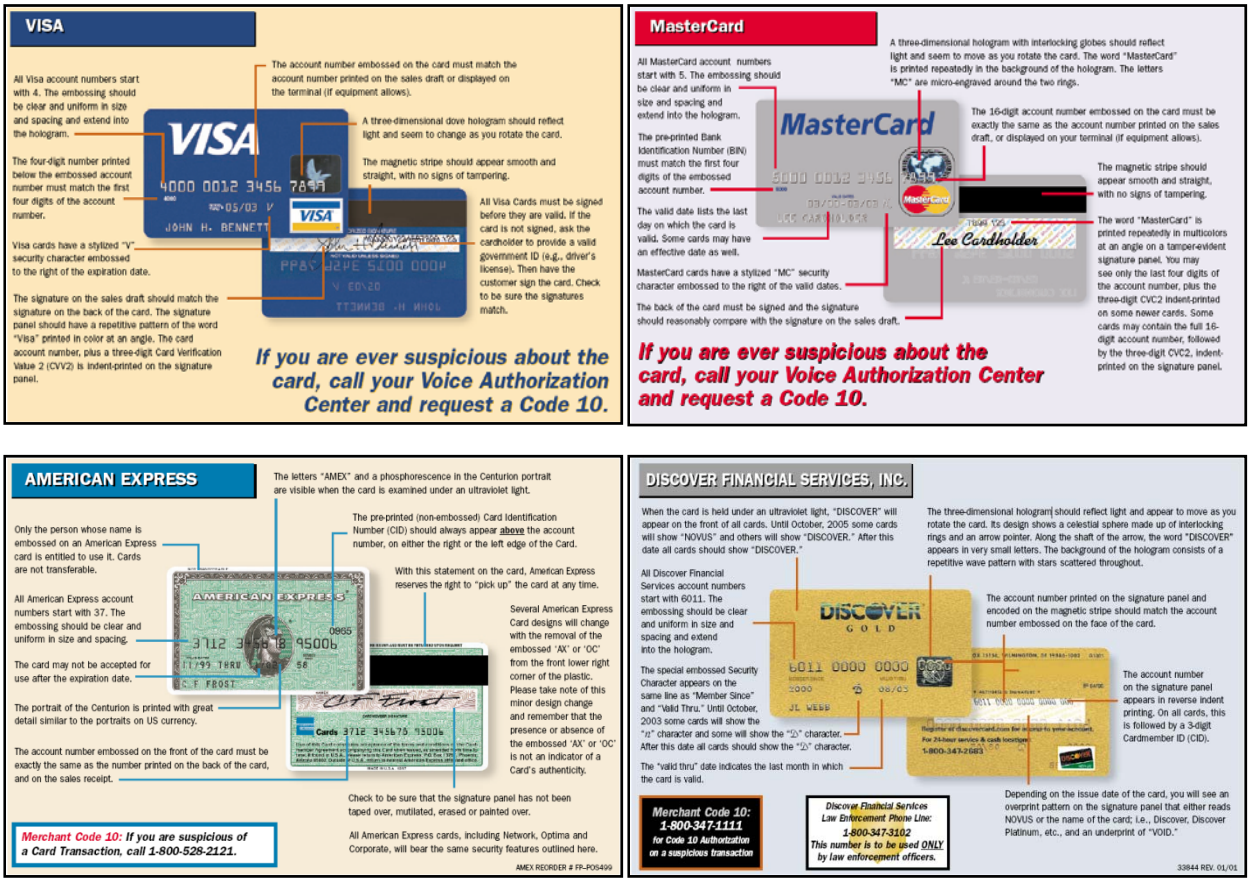


1. In this case, when we sum up the total, it comes to 61 which is *not* perfectly divisible by 10, and hence this credit card number is invalid.

2. If such a credit card number is ever generated, the value of the check digit would be adjusted in such a way as to satisfy the Luhn condition. In this case, the only value of the check digit, that will create a valid credit card number, is 7. Choosing 7 as the check digit will bring the total to 60 (which is perfectly divisible by 10) and the Luhn condition will be satisfied. So the valid credit card number will be **4552 7204 1234 5677**.

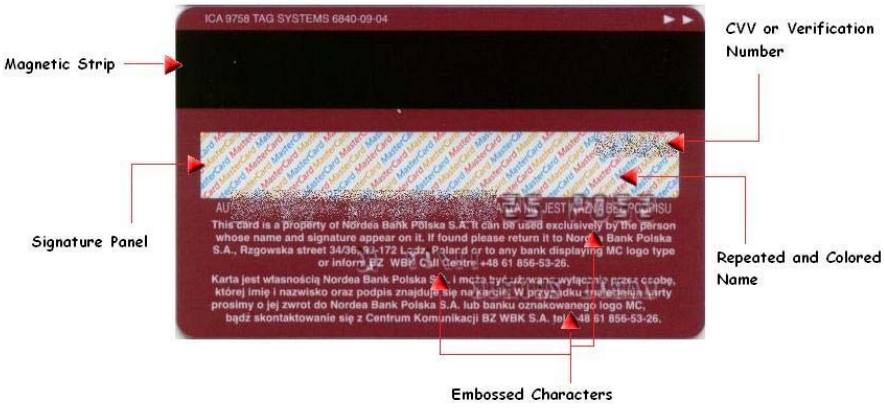
## Credit Card Features

There are other ways to detect a fraudulent credit card. The four boxes below describe the various attributes that appear on each of the four major types of credit cards.




## Credit Card Security Measures

The low security of the credit card system presents countless opportunities for fraud. This opportunity has created a huge black market in stolen credit card numbers, which are generally used quickly before the cards are reported stolen. The goal of the credit card companies is not to eliminate fraud, but to "reduce it to manageable levels".




To make credit cards more secure, the following security measures are commonly available:

1. **The Card Security Code (CSC)** - Sometimes called Card Verification Value or Code (CVV or CVC), is a security feature for credit or debit card transactions, giving increased protection against credit card fraud. There are actually two security codes:

    a. The first code, called CVC1 or CVV1, is encoded on the magnetic stripe of the card and used for transactions in person.

    b. The second code, and the most cited, is CVV2 or CVC2. This CSC (also known as a CCID or Credit Card ID) is often asked for by merchants for them to secure "card not present" transactions occurring over the Internet, by mail, fax or over the phone. In many countries in Western Europe, due to increased attempts at card fraud, it is now mandatory to provide this code when the cardholder is not present in person. An additional 3 or 4 digit code is provided on the back of most credit cards, for use in "card not present" transactions.

    **CVV2's Are Encrypt Generated -** These numbers are generated when the card is issued, by encrypting the card number and expiration date under a key known only to the issuing bank. Supplying this code in a transaction is intended to verify that the customer has the card in their physical possession. To date, no cracks for this system are known.

    **CVV2's Vulnerable to Phishing** - The use of the CVV2 cannot protect against phishing scams, where the cardholder is tricked into entering the CVV2 among other card details via a fraudulent website.

    **CVV2's May Not Be Stored –** By rule, CVV2 may not be stored by the merchant for any length of time (after the original transaction in which the CVV2 was quoted and then authorized and completed); therefore, a merchant who needs to regularly bill a card for a regular subscription would not be able to provide the code after the initial transaction.

2. **Photo Security** – The cardholder's picture is now affixed to many credit cards. However, the logistical complications of taking a photo, verifying the photo, and affixing it to a person's credit card are still too burdensome to require this of all credit cards at this time.


3. **Transaction Monitoring** – Credit card companies look for red flags such as:

    a. Shipping address is different from the billing address. Or the shipping address has suddenly changed.
    b. Unusually large purchase compared to normal purchase patterns for the account in question.
    c. Change in name on the account.
    d. Change in date of birth or social security number.
    e. Unusual purchases over the Internet.
    f. Unusually high number of transactions.

4. **PINs** - The on-line verification system used by merchants is being enhanced to require a 4 digit Personal Identification Number (PIN) known only to the card holder.

5. **Improved Material** – Credit cards are now being replaced with similar-looking tamper-resistant smart cards which are intended to make forgery more difficult. The majority of smartcard (IC card) based credit cards comply with the EMV (Europay MasterCard Visa) standard.

## Paying the Minimum Balance

While not really a security risk, it should be noted that paying the minimum balance on a credit card statement can cost you far more than most security risks. Therefore I will comment briefly on this topic as follows:

The table below shows what would happen if you have a $5,000 outstanding balance on your credit card (to keep things simple, we assume you make no additional purchases), an Annual Percentage Rate (APR) of 18 percent, and you make only the minimum payment due ($100 initially but gradually declining each month because minimum payments usually are based on a percentage of the balance, which will decrease.) Using this example, it will take 46 years and cost $13,926 in interest charges before you've paid the $5,000, putting the total cost at $18,926.

**Making Only the Minimum Payment Adds to Costs**

| Starting Balance | Interest Rate (APR) | Monthly Payment | Years to Pay Off | Total Interest Paid | Total Cost |
|---|---|---|---|---|---|
| $5,000 | 18% | The minimum ($100 the first month, then gradually declines) | 46 | $13,926 | $18,926 |
| $5,000 | 18% | $100 | 8 | $4,311 | $9,311 |
| $5,000 | 18% | $250 | 2 | $986 | $5,986 |

Note: The minimum payment is assumed to be two percent of the outstanding balance or $10, whichever is greater. Years are rounded to the nearest whole year.

## Easy Credit Cards for College Students

Credit card companies target college students more than any other single group –because college students are excellent targets for running up high bills, paying minimum balances, and having the resources to eventually pay off the entire debt. More importantly, these companies want to lock college students in now to using their card brand so they can leverage their future earnings potential. Upon entering college, you child will be barraged with credit card applications and you need to help make sure that they do not fall into this common trap.

## Credit Card Dead Beats

In the credit card industry, people who pay off their entire credit card balance each month are called dead beats. They are dead beats to the credit card issuers because they generate far less revenue to the credit card companies than do people who pay the minimum balance.

## Common Credit Card Scams

While theft is the most obvious form of credit and charge card fraud, it is not the only way fraud occurs. A more subtle form of fraud is misappropriation. The use of your card number (not the card itself) without your permission. Misappropriation may occur in a variety of ways. Examples are:

1. A phone caller says that you need only provide your card number and its expiration date to qualify for a special discount vacation.
2. A thief rifles through trash to find discarded receipts or carbons to use the card numbers illegally.
3. A dishonest clerk makes an extra imprint from your credit or charge card for his or her personal use.

Fraudulent credit card information or credit cards themselves are usually obtained through:

1. Fake Web Sites
2. Theft
3. Pick Pocketing
4. Phishing
5. Credit Card Swapping at ATM Machines
6. Skimming

**Security Tips for Employees -** While the following measures are fairly obvious, you should make sure that your employees follow the guidelines set forth below to help protect your company from credit card fraud:

1. Hide keypad when entering a PIN at an ATM.
2. Don't leave your receipt behind at the ATM.
3. Destroy expired cards.
4. Immediately sign new cards.
5. Don't keep your PIN numbers in your wallet.
6. Treat credit cards as if they were real money.
7. Lost or stolen cards should be reported immediately.
8. Be cautious when giving credit card information to websites or unknown individuals.
9. Verify transaction on your credit card statement with your receipts.
10. Keep an eye on the credit card when making transactions in shops.
11. Don't sign a blank credit card receipt.
12. Don't loan credit cards to other employees.
13. Always keep a list of your credit cards, credit-card numbers and toll-free numbers in case your card is stolen or lost.
14. It doesn't matter whether or not their website is encrypted. Encryption means that your data is secure between your computer and the merchant, not between your computer and the credit card processor. The merchant will have your card number regardless. If you're buying from an unfamiliar or likely untrustworthy store, consider using a temporary/virtual card number that card companies like Citibank provide.

**Security Tips for Merchants -** Watch out for suspicious behavior of your customers. Some characteristics are in common with fraudulent transactions, although none of this can be an actual proof of credit card fraud it still remains a good measure of identifying suspicious behavior. This type of fraud can eat up your profits so watch out when a customer:

1. Buys a priced item on a new credit card.
2. Purchases large amounts of expensive items and doesn't seem to care for other amounts that can occur during the transaction (delivery, packaging...).
3. Making small purchases to stay under the floor limit.
4. Asks what the floor limit is.
5. Making random purchases with no regard size, price or quality.
6. Takes the credit card out of his pocket instead of a wallet.
7. Awkwardly or slowly signs the receipt.
8. If asked, cannot provide a photo ID.
9. Credit card validation date expired.
10. Credit card seems counterfeited or information altered.
11. Receipt signature differs from the one on the card.

**Common Types of Credit Card Fraud -** What are the common types of credit card fraud? Counterfeit Credit Cards, Account Take Over and Skimming. We are going to look at each one and describe it.

1. **Account Take-Over –** A thief does not need your credit card to empty your bank account, all he needs is your personal credit card information. He will typically phone your credit card company and change your address information. He will then report the credit card as stolen and request a new credit card; or he will order a second credit card while pretending to be you. This card will then be sent to the new address. Your statements also will be sent to this new address, making you unaware of the fraud. Therefore, if you don't get statements on a monthly basis at about the same day, you should contact your financial institution and check your records on file. Ask for address change or if any information has been changed without your direct approval.

2. **Mail Box Theft** - A thief will steal your new credit card when it still is in your postal box or anywhere on the way between the bank and you. This can be an organized crime scenario involving assistants, such as a postman who intercepts your mail before it is delivered to your address. A fraudster may even get a hold of information when credit cards are issued to a particular address, waits near your mailbox and takes your mail. So if you get a notification about an important delivery, collect it as soon as possible, because the longer you wait, the bigger the chance for a fraudster to intercept it.

3. **Counterfeit Credit Cards -** Counterfeit or altered credit cards is in short, duplicating legitimate credit cards which are then used for fraudulent activities. The latest technology is used in accordance with lamination and embossing to create realistic

looking credit cards. To the untrained eye these will appear real and you will not be able to recognize the difference, since a complete hologram as well as the magnetic strip is included in the fake credit card.

4. **Credit Card Skimming -** Electronic card readers, or Skimmers, are used in stores legitimately when processing a transaction. However in the hands of a thief such a tool can be used to gather information for later usage in criminal activities. Usually a small electronic device is plugged into the real electronic reader and now gathering information of everyone who purchased at the store or done a money request at the ATM machine. Or a portable skimmer is used to quickly swipe your card through the magnetic reader while you are not looking. Such information will be used for later unauthorized purchases or making of a new counterfeit credit card. Usually done in restaurants or similar institutions where you usually temporary lose sight of your credit card.


A typical skimming device is about the size of a pager, connected in the phone-line between the phone-jack and credit card machine. A modern "skimmer" costs about $300, compared to the $5,000-$10,000 in equipment needed to make a counterfeit credit card. When customers make a purchase, their cards are swiped through the business's credit-card machine, where the card data is read from the magnetic strip and phoned in for approval. During this normal approval process, the "skimmer" captures the data and either duplicates it onto the mag-strip of plastic credit-card "blank", or stores it within the skimming device to be downloaded later. *(* —The magnetic stripe on credit cards is a "passive media", allowing creation of perfect copies of the digital credit card content.)*


Credit card skimming can also occur any time that your card leaves your direct possession. Another common skimmer-scam involves locating a portable skimmer card-swipe device near the business's own card-scanner, or even a portable device carried in the pocket of a server. For example, your server brings your bill on the tip-tray at the end of your meal. You place your credit card on the tip-tray and the server returns to take your card/bill to the register for you. When your card is swiped through the business's card-reader to approve your "authorized" purchase, it's also secretly swiped through a "skimmer" to steal your card's data, then the server returns your card to you.

In both these methods, the restaurant employee is a thief — either later using your card data fraudulently, or simply paid a flat rate *(per card)* by a thief for obtaining card data.

Many skimmers are even equipped with a *panic button* to instantly erase all collected data, eliminating all evidence in case of discovery.

An example: In the summer of 1999, two New York City restaurant servers were charged with skimming more than $300,000 from unsuspecting patrons.

Another type of high-tech skimmer can be secreted **inside** a business's normal credit cardreader, and includes a **wireless transmitter** that allows skimmed numbers to be secretly recorded on a laptop computer anywhere within about 300 feet. *(With this device, a thief can sit outside the restaurant in a car, skimming numbers, and no one may ever connect him with the crime.)* Unless the restaurant staff notices someone has tampered with their cardreader, the crime may not be discovered for quite some time!

A new and potentially far more dangerous form of point-of-sale terminal skimming involves implanting sophisticated ***software*** "skimmer bugs" into cardreader terminals *(and tiny "hardware" bugs for older terminals)*, allowing stolen information to be sent over the phone lines of legitimate swiping machines. These "skimmer bugs"" can store numbers within the circuitry in the device and simply use the cardreader's modem to dial out to a computer where the thief thief-system uploads the numbers. A few days later, the thief can even remove the bug, leaving virtually no sign there has ever been any tampering.

Annual U.S. skimmer-related losses exceed $100 million, and have grown from 3 percent just a few years ago to presently accounting for over 25% of all fraud involving high-tech devices.

*"Skimming is the biggest problem in bank fraud today,"* says Gregory Regan, head of the U.S. Secret Service Financial Crimes Division. *"It's the bank robbery of the future. It's technically simple, point-and-click technology. And the equipment is cheap. If you skim 15 or 20 accounts, you can generate $50,000 to $60,000 worth of fraud, and nobody is going to know about it until the victims get their bills, 30 to 60 days after the crime. So the odds of getting caught are reduced."*


# Counterfeit Money

## Chapter 36

# Counterfeit Money

# How to Detect Counterfeit Money

1. **Compare** - Compare a suspect note with a genuine note of the same denomination and series, paying attention to the quality of printing and paper characteristics. Look for differences, not similarities.

2. **Feel the Paper -** US bank notes are printed on special paper that's 75% cotton and 25% linen. The linen gives it an extra stiffness that's distinctive.

3. **Color Shifting -** Bank notes bigger than the $5 use color-shifting ink to print the number showing the denomination in the lower-right-hand corner. Just look at the numbers head-on, and then from an angle. For genuine notes the color will shift (copper-to-green or green-to-black).

4. **Portrait -** The genuine portrait appears lifelike and stands out distinctly from the background. The counterfeit portrait is usually lifeless and flat. Details on fake bills usually merge into the background which is often too dark or mottled.

(Real)  (Fake)

5. **Federal Reserve and Treasury Seals -** On a genuine bill, the saw-tooth points of the Federal Reserve and Treasury seals are clear, distinct, and sharp. The counterfeit seals may have uneven, blunt, or broken saw-tooth points.

(Real)  (Fake)

6. **Border -** The fine lines in the border of a genuine bill are clear and unbroken. On the counterfeit, the lines in the outer margin and scrollwork may be blurred and indistinct.

(Real)  (Fake)

7. **Serial Numbers -** Genuine serial numbers have a distinctive style and are evenly spaced. The serial numbers are printed in the same ink color as the Treasury Seal. On a counterfeit, the serial numbers may differ in color or shade of ink from the Treasury seal. The numbers may not be uniformly spaced or aligned.

(Real) 

(Fake)

8. **Paper Fibers -** Genuine currency paper has tiny red and blue fibers embedded throughout. Often counterfeiters try to simulate these fibers by printing tiny red and blue lines on their paper. Close inspection reveals, however, that on the counterfeit note the lines are printed on the surface, not embedded in the paper. It is illegal to reproduce the distinctive paper used in the manufacturing of United States currency.

(Real)  (Fake)

9. **Watermark -** All bills bigger than a $2 now have a watermark--hold the bill up to the light to see it. For the $10, $20, $50, and $100, the image matches the portrait. That's also true of the current $5 bill, but on the new $5 which came out in 2008, the watermark is a big numeral 5.

10. **Security Thread -** All bills bigger than a $2 have a security thread running vertically through the bill. Like the watermark, you hold the bill up to the light to see it

11. **Raised Notes -** Genuine paper currency is sometimes altered in an attempt to increase its face value. One common method is to glue numerals from higher denomination notes to the corners of lower denomination notes. These bills are also considered counterfeit, and those who produce them are subject to the same penalties as other counterfeiters. If you suspect you are in possession of a raised note:


a. Compare the denomination numerals on each corner with the denomination written out at the bottom of the note (front and back) and through the Treasury seal.

b. Compare the suspect note to a genuine note of the same denomination and series year, paying particular attention to the portrait, vignette and denomination numerals.

12. **Counterfeit Detector Pens** - Counterfeit detector pens (like the one shown below from Risk Reactor) will help you spot counterfeit bills. Simply use the pen to draw a line or dot across the bill. If the line or dot stays amber, the currency is genuine; if it turns black, the money will be counterfeit. Marks fade to keep bills clean and useable.

**Counterfeit Coins**

1. **Poured** - Genuine coins are struck (stamped out) by special machinery. Most counterfeit coins are made by pouring liquid metal into molds or dies. This procedure often leaves die marks, such as cracks or pimples of metal on the counterfeit coin.

(Real)   (Fake)

2. **Rare** - Today counterfeit coins are made primarily to simulate rare coins which are of value to collectors. Sometimes this is done by altering genuine coins to increase their numismatic value. The most common changes are the removal, addition or alteration of the coin's date or mint marks.

**Death Penalty for Counterfeiting -** The Coinage Act of 1792 mandates the DEATH PENALTY for DEBASING the currency. Read for yourself…

> " And be it further enacted, That if any of the gold or silver coins which shall be struck or coined at the said mint shall be debased or made worse as to the proportion of the fine gold or fine silver therein contained, or shall be of less weight or value than the same out to be pursuant to the directions of this act, through the default or with the connivance of any of the officers or persons who shall be employed at the said mint, for the purpose of profit or gain, or otherwise with a fraudulent intent, and if any of the said officers or persons shall embezzle any of the metals which shall at any time be committed to their charge for the purpose of being coined, or any of the coins which shall be struck or coined at the said mint, every such officer or person who shall commit any or either of the said offenses, shall be deemed guilty of felony, and shall suffer death" (Section 19).

**Photographing Money or Checks**


The law sharply restricts photographs or other printed reproductions of paper currency, checks, bonds, revenue stamps and securities of the

United States and foreign governments. Specifically, the Counterfeit Detection Act of 1992, Public Law 102-550, in Section 411 of Title 31 of the Code of Federal Regulations, permits color illustrations of U.S. currency provided:

- The illustration is of a size less than three-fourths or more than one and one-half, in linear dimension, of each part of the item illustrated.

- The illustration is one-sided.

- All negatives, plates, positives, digitized storage medium, graphic files, magnetic medium, optical storage devices, and any other thing used in the making of the illustration that contain an image of the illustration or any part thereof are destroyed and/or deleted or erased after their final use.


**Photographing Foreign Money -** Photographs or reproductions of foreign currencies are permissible for any non-fraudulent purpose, provided the items are reproduced in black and white and are less than three-quarters or greater than one-and-one-half times the size, in linear dimension, of any part of the original item being reproduced. Negatives and plates used in making the likenesses must be destroyed after their use for the purpose for which they were made. This policy permits the use of currency reproductions in commercial advertisements, provided they conform to the size and color restrictions.

**Counterfeit U.S. Postage Stamps**

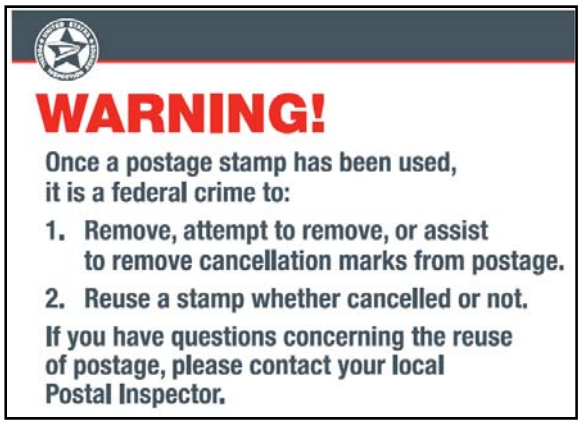
**2008 Bust -** In February 2008, an underground printing operation in New York City was caught producing $300,000 worth of high-quality counterfeit U.S. postage stamps. The U.S. Postal Inspection Service says such operations are just a small part of a thriving black market in bogus stamps. The busted printing operation was being run out of an apartment on the Upper West Side of Manhattan.

Counterfeit U.S. Postage Stamps

In the raid they also found USPS wrappers complete with barcodes, computer software, industrial-sized cutting boards, three industrial printers and other professional printing supplies. Authorities say the quality of the counterfeit stamps was excellent and that they were destined to be sold at cut rates on the Internet or at small grocery stores in New York. The US Post Office reported that people most often sell counterfeit stamps online and door-to-door.

**Phosphor Security Feature -** The investigation into counterfeit stamps was triggered after postal inspectors discovered that hundreds of letters were being rejected for delivery because the stamps lacked the required phosphor tagging.

**It is Illegal to Reuse Stamps –** According to the US post Office web site, it is illegal to reuse a stamp that has already been used, even if that stamp was not properly cancelled. Here is the excerpt:




**Counterfeit Tax Stamps**

Also in February 2008, millions of dollars worth of counterfeit cigarette tax stamps were seized in New York, authorities announced Wednesday. The fake stamps would have allowed unscrupulous cigarette dealers to evade nearly $6.1 million in state and city taxes. Tax stamps,

which must be affixed by distributors to packs of legal cigarettes, cost $3 each in New York City, $1.50 in the rest of the state and $2.57 in New Jersey.


## Security Features of U.S. Treasury Checks

Counterfeiting of checks issued by the Federal Government has become a common problem. Accordingly, several security features have been incorporated into U.S. Treasury checks that are easy to authenticate and difficult to reproduce on office machine copiers/printers, as follows:


1. **Paper -** The paper used for Treasury checks is chemically responsive to all solvents and ink removers, which make most alterations easy to notice. It also contains a continuous pattern watermark that says "U.S. Treasury." This security feature cannot be reproduced on an office machine copier.

2. **Printing -** The dry offset printing process is used to print Treasury checks. The inks react to leaching and bleaching. They fade when rubbed with water and dissolve when exposed to alcohol or bleach. This makes most alterations noticeable.

3. **Copy-Proof Colors -** The colors of the inks are of a low density, which makes them difficult to reproduce on an office machine copier.

4. **Microprinted Text -** The signature line on the reverse side of the check is comprised of microprinted text that repeats the letters "USA."

5. **Fluorescent Image** - The checks have a fluorescent image printed in the center that can be viewed under ultra-violet light but cannot be reproduced by an office copier.

6. **Bleeding Ink -** Bleeding ink in the Treasury Seal, which will smudge red when exposed to moisture.

7. **Dual Wavelength Bands** - The fluorescent image overprinted in the center has been enhanced to contain dual fluorescent wavelength bands.

**Alterations Forfeit the Entire Government Check -** If a legitimate payee alters the amount on a government check, they forfeit the entire original amount of the check and are subject to criminal prosecution.

**Fake $1 Million Bill** – In 2004, a Covington, Ga. woman tried to use a fake $1 million bill to buy $1,675 worth of merchandise at Wal-Mart said it was all just a misunderstanding — she thought the bill was real. Her estranged spouse gave joke-shop currency to her.

# Cracking and Hacking

## Chapter 37

# Introduction

Hacking, Cracking, and Phreaking are alive and well today. The Internet provides the communication pipeline that allows tens of thousands of hackers, crackers, and phreakers to share information and teach one another how to bust into the latest hardware, local area networks, operating systems, and software application products. Today, anyone with a desire to do so, can become a hacker, cracker or phreaker and try their hand at hacking, cracking, or phreaking. Just so you know:

1. The term "Hacker" refers to non-destructive, law-abiding people who are expert programmers and systems wizards. They fancy themselves as "computer gurus" who use their talents to make things work. You are not considered to be a "hacker" until other "hackers" routinely refer to you as a "hacker". Being a "hacker" is supposed to be "COOL".

2. The term "Cracker" refers to destructive people who use their hacking skills (or hacking tools) to break into systems, destroy systems, steal data, rip off application software, and perform a number of illegal activities. Being a "Cracker" is supposedly "CRIMINAL".

3. The term "Phreaker" refers to people who break into telephone systems in order to call long distance with no charge, to tap phone lines, to break into voice mail boxes, to steal information, to eaves drop, to cause damage, etc. Being a "Phreaker" is supposedly "CRIMINAL".

# Why Study Hacking, Cracking & Phreaking?

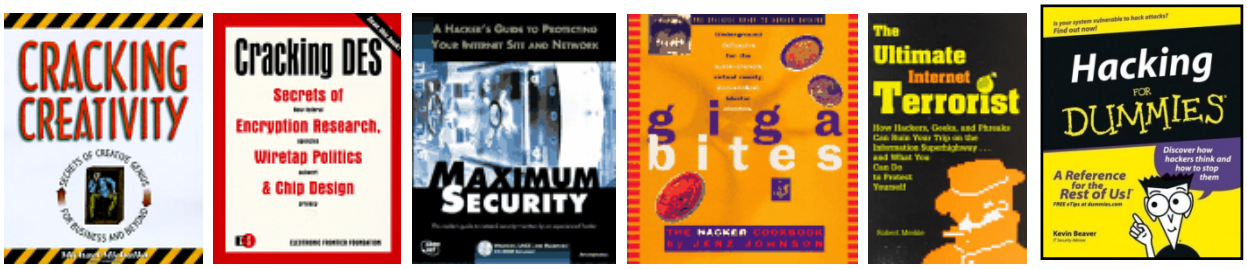
The fact that virtually any intelligent person can easily become a hacker, cracker, or phreaker posses a security threat to every organization. Today's Systems Information professionals need to be aware of the type threats that exist today in order to take the necessary measures to protect against these threats. In some cases, System Information Professionals can use the same tools the crackers use in order to test the security of their own systems. In other cases, knowledge in this area can help the Systems Information Professional identify employees or others who may be openly discussing these tools, searching for these tools, or downloading these tools in time to take corrective measures. Further an understanding of these threats is necessary to help Systems Information Professionals develop policies and procedures to help prevent problems before they arrive.

### Key Hacking & Cracking Terms:

| Term | Example Web Sites |
|---|---|
| A. Hacking (42,000,000) | http://the-hacking-community.iscool.net/<br>http://catb.org/~esr/faqs/hacker-howto.html |
| B. Cracking (25,600,000) | http://packetstorm.securify.com/Crackers/<br>http://www.antionline.com/cgi-bin/anticode/anticode.pl<br>http://www.ovnet.com/~p80/sample.htm |
| C. Phreak, Phreaking, Phrack (1,060,000) | http://www.phrack.com/archive.html |
| D. 40Hex (4,660) | http://www.fc.net/phrack/under/40hex.html |
| E. Serialz (serial numbers) (4,640,000) | http://home.global.co.za/~odge/serialz.htm<br>http://www2.50megs.com/cpage/ |
| F. Crackz (cracking programs) (5,360,000) | http://www.crackstore.com/index2.htm<br>http://www.strega.org/zor/index.html |

| | |
|---|---|
| G. Hacking Tools (1,270,000) | http://www.8bn.com/jtb/ |
| H. Hacking Magazines (444,000) | http://www.2600.com/ |
| I. E-Mail Tools (11,500) | http://www.onworld.com/MUT/mutForum/messages/2913.html |
| J. Anonymous Senders (381,000) | http://help.mindspring.com/modules/g0000/g0086.htm<br>http://www.ecn.org/crypto/remailer/<br>http://nogov.org/Anonymous/<br>http://www.users.globalnet.co.uk/~firstcut/remail.html<br>http://www.interlink-bbs.com/anonremailer.html |
| K. Bombers (11,000,000) | http://www.escalix.com/freepage/freeworld/mailbomber.htm |
| L. Key Generators (1,540,000) | http://home.luna.nl/~enigma/tex/ |
| M. Flooders (411,000) | http://www.antionline.com/cgi-bin/anticode/anticode.pl?dir=denial-of-service |
| N. Cracking Search Engine | http://astalavista.box.sk/ |
| O. ICQ Tools (112,000) | http://www.antionline.com/cgi-bin/anticode/anticode.pl?dir=icq |
| P. Sniffing Tools (163,000) | http://www.bellacoola.com/<br>http://www.licht-labs.com/sniffer.html<br>http://www.lachniet.com/maeds/sld013.htm |
| Q. Key Loggers (397) | http://ftp.castel.nl/~groor01/tools.htm |
| R. Spoofing Tools (146,000) | http://www.licht-labs.com/ipspoof.html |
| S. Fake Ids (254,000) | http://www.chattownusa.com/Avenues/Teen/idfu/<br>http://serialns.8m.com/cgi-bin/framed/1940/samples.html<br>http://www.4.hactivist.net/<br>http://www.4.hactivist.net/<br>http://www.prestigious-images.com/docs.html#ssa |
| T. Credit Card Making Equipment (453,000) | http://www.4.hactivist.net/<br>http://www.idhouse.com/idsoft.htm<br>http://www3.sympatico.ca/the.chaser/CARD.HTM |
| U. Learning to Hack | http://www.zerberus.de/texte/ccc/ccc95/artikel/hackan_e.htm |
| V. Hacked Sites | http://www.2600.com/hacked_pages/prop/ |
| W. Meetings | http://www.2600.com/meetings/<br>http://www.dnai.com/~waxwing/wwwboard/messages/212.html |
| X. Hacking and Cracking terms in different languages | ftp://sable.ox.ac.uk/pub/wordlists/<br>http://www.pfu.co.jp/hhkeyboard/ |
| Y. Foreign Language Conversion | http://babel.altavista.com/translate.dyn?urltext=http%3a%2f%2fwww%2eaccountingsoftwarenews%2ecom%2f&language=en |
| Z. DIRT (virus) (44,000) | http://www.netsurf.com/nsd/v05/nsd.05.21.html |

## Hacking, Cracking and Phreaking Books




There are plenty of books available on the subjects of Hacking, Cracking and Phreaking. For example, the book **Maximum Security** was written by an anonymous hacker to help you protect your system from invaders and the arsenal of tools, back-end secrets, and bugs they have at their disposal. We don't know much about the author of *Maximum Security*--only that he was convicted of multiple crimes involving friendly neighborhood ATM systems before deciding to use his talents in a more law-abiding fashion. Told from a hacker's perspective, *Maximum Security* details methods for concealing identity, cracking passwords, and gaining access to systems running everything from Unix to Windows NT to the Mac OS. He also explains how best to counter or prevent these techniques. Every system administrator should read this book and sleep better at night for having done so.

## How Easy Is It To Become A Cracker?

Simply search the Internet for a file called "40HEX". You will find it available on thousands of web sites. This file contains 40 deadly viruses, along with instructions for altering these viruses to make them more deadly. From here, you could simply send these files to an unsuspecting person via a diskette, e-mail, or web page downloadable file. The diskette, e-mail message, or web page could assert that the file will clean up a hard drive - thereby making your system run up to 30% faster. Many suckers would fall victim to such a scheme.


There are also guides, tutorials, text books, and lessons all designed to help you learn how to become a Cracker. All you need do is search the Internet for the term computer cracker, and you will find over 579,000 web sites with information on the subject - incredible. Because of the criminal nature of these web sites, they are constantly moving from one web server to another as they are censured by their web page hosting service or as law suits are filed against the owners of these web sites. Still, these crackers seem to simply move their web site to a new server

for a few months, announcing their moves in the cracker chat rooms and discussion groups. Censuring these web sites is akin to herding cats - it's probably not going to happen.

## Why Do Hackers Hack and Crackers Crack?

Hackers generally hack for money. They are generally available for hire to write code, test code, test systems, implement firewalls, etc. The problem is that based on many of the web sites I have visited, many Hackers are also Crackers - although there appears to be a well established movement among Hackers to denounce cracking activities. As shown below, 90% of all hackers are considered to be amateurs - which means they really haven't earned the right to be called a hacker - but they are working at it.

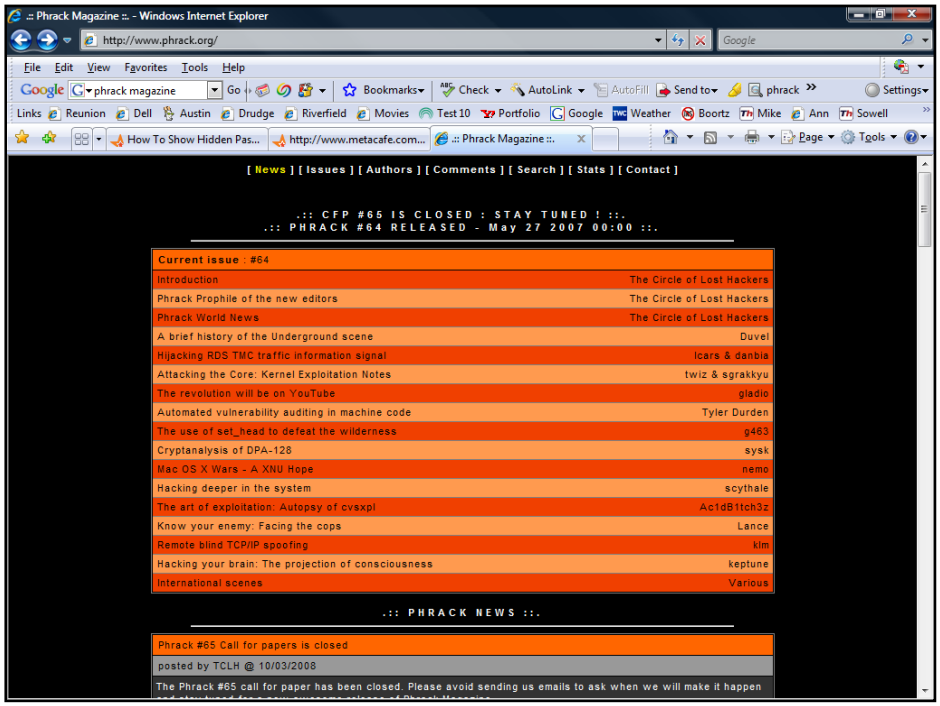

Crackers appear to crack for several different reasons as follows:

> Just as you and I play chess for the sheer intellectual challenge of the game, some crackers crack for the sheer challenge as well. It is as if some expert out there has established security defenses and stated "*I dare you to break through these defenses*". Some crackers enjoy breaking through this security and have no evil intentions of stealing data or destroying data once they have achieved their goal. They obtain immense satisfaction in having proven their skill to oneself.
>
> Other Crackers are just plain evil and they get a kick out of sabotaging someone's systems, destroying their data, or otherwise making someone's life miserable. Trying to understand this motive is akin to understanding why a juvenile smashes mail boxes - it's just plain stupid and most mature people see it that way.
>
> Many crackers crack in order to save money. Instead of purchasing the latest software, they simply steal it, copy it, or break through the evaluation copy defenses. Crackers also attempt to obtain free access to the internet, pay-per-view web sites, and subscription web sites.
>
> The final reason a Cracker cracks is for money. Some professional crackers crack in order to steal information that they can use or sell - almost always in a criminal manner. For example, a list of names, addresses and credit card numbers would be easy to sell on the black market as evidenced by the fact that credit card making machines and blanks are widely available through cracking web sites. At least the motive is plain to see and easy to understand.

## Why Do Phreakers Phreak?

Phreakers phreak for the same reasons that crackers crack - some for the challenge, others to cause havoc, some to avoid phone charges, and yet others are looking for information that can be used to turn a profit. It also appears that phreaking technology is used moderately by private detectives and possibly company security officials who

want to keep an eye on someone. Learning to Phreak is as simply as visiting Phrack magazine located at: http://www.phrack.org/




Here you will find hundreds of detailed articles describing how to break into phone systems, make long distance calls without being charged, build equipment that can be used to tap a phone, purchase a device that let's you dial any phone number in the world, the phone you dial will not ring, but then you can listen to the conversations going on in the room. Using this information, any employee, customer or person with access to your conference room could eaves drop in on your next Board of Directors meeting.

## Sample Hacking, Cracking & Phreaking Web Sites

This page provides a basic introduction to hacking - http://catb.org/~esr/faqs/hacker-howto.html.

Hacking runs the gambit from harmless pranks to vicious breaches of security. For example, one web site explains how to edit the Windows XP host file to get Internet Explorer point to point to a different web site other than the one entered. Here are the steps:

1. Visit www.ipaddress.com and obtain the IP address for the target web site.
2. Search for the file called “hosts" (in Windows Vista, XP and 2000 it is in C:/windows/system32/drivers/etc/.)
3. Open the Hosts file with NotePad.
4. Add this text to the bottom: 206.61.52.30 www.cia.gov.
5. In the future, typing in www.cia.gov will instead take the user to the web site 206.61.52.30, but the URL will still read www.cia.gov.
6. You will need administrator rights to edit the Hosts file.

## Famous Hacking Web Site

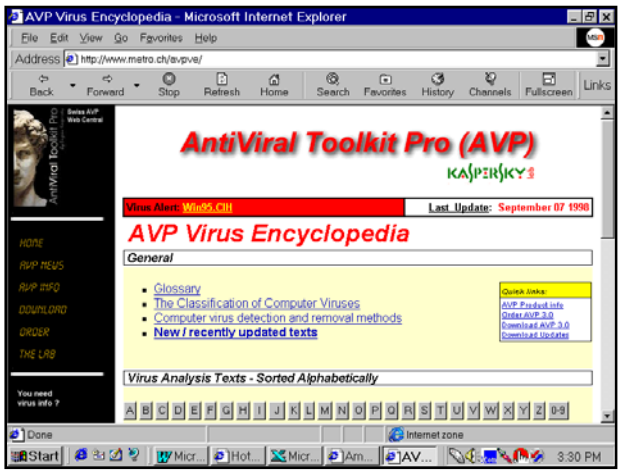

http://www.2600.com/mindex.html - 2600 The Hacking Quarterly.

## Cracking and Hacking Tools

There are hundreds of tools that you can download free of charge and use for hacking, cracking, and phreaking. CAUTION - If you download any of these files you should run them only on a single user computer - do not run them on a workstation on your local area network. You should scan all files for viruses - first making sure that you have the latest version of your virus protection software. You should be advised that the use of some of these tools may constitute illegal activity and could cause damage inadvertently to your company's computer systems for with you could go to jail. Please be careful and take all of the necessary cautions before downloading any of the files discussed below:

# Viruses

Viruses come in many different flavors including, Boot viruses, File viruses, Macro viruses, Multipartite viruses, NewExe viruses (Windows95, Windows, OS/2, Unix), Trojans, Virus Constructors, and Joke programs. You can keep track of the latest list of known viruses including detailed descriptions of those viruses at many web sites including McAfee, Dr. Solomon, Norton AntiVirus, and the AVP Virus Encyclopedia web site shown below:




Viruses are divided into classes according to the following four characteristics:

1. Environment;
2. Operating system (OS);
3. Different algorithms of work; and
4. Destructive capabilities.

The environment of a virus may affect either the file; boot; macro; or network. File viruses infect executables. Boot viruses save themselves in disk boot sector or to the Master Boot Record. Macro viruses infect document, spreadsheets, and databases files. Network viruses use protocols and commands of computer network or e-mail to spread themselves. Each file or network virus infects files of one particular or several Operating Systems such as DOS, Windows 3.xx, Windows95/NT, OS/2 etc. Macro viruses infect the Word, Excel, Office97 format files. Boot viruses are also format oriented, each attacking one particular format of system data in boot sectors of disks. Among OPERATING ALGORITHMS the following features stand out: TSR capability; the use of Stealth algorithms; self encryption and polymorphic capability; and the use of non-standard techniques. A viruses destructive capabilities can be divided as follows:

1. Harmless,
2. Not dangerous, limiting their effect to lowering of free disk
3. Dangerous, which may seriously disrupt the computer's work;
4. Very dangerous, the operating algorithms intentionally contain routines which may lead to losing data, data destruction, or erasure of vital information in system areas.


Many of the hacking, cracking, and phreaking tools are really just instructions rather than actual programs you download and run. For example, assume that your client's bookkeeper quit but before they left, they inserted a new password into QuickBooks. Your client can no longer access their data and the disgruntled employee is long gone. In this case, hackers have solved this problem and the instructions are readily available on the Internet, as shown in the screen below:

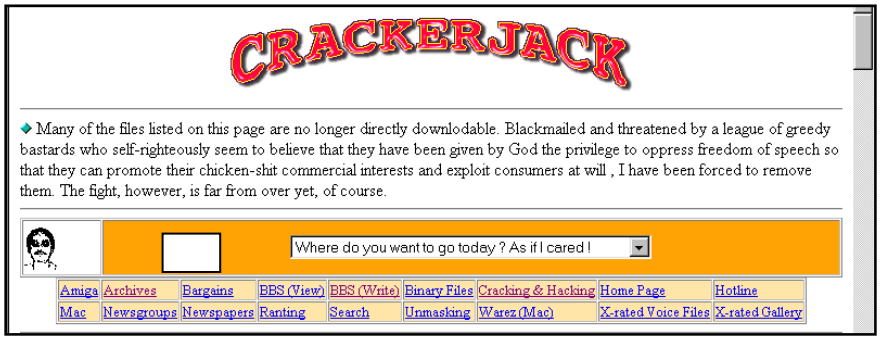
In this case, this web site called Password Recovery Tactics describes the procedure in which you can use Norton's Tools to peek into the hexadecimal code for QuickBooks and replace the encrypted password with your own password. Notice that while this example appears to be a hackers constructive use of this information, an evil employee or other person could use this information to access confidential financial data. The borderline between hacker and cracker is very narrow indeed.

**SATAN** - (Security Analysis Tool for Auditing Networks). In default mode, SATAN gathers as much information about remote hosts and networks as possible by examining such network services as finger, NFS, NIS, ftp and tftp, rexd, and other services. The information gathered includes the presence of various network information services as well as potential security flaws -- usually in the form of incorrectly setup or configured network services, well-known bugs in system or network utilities, or poor or ignorant policy decisions. It can then either report on this data or use a simple rule-based system to investigate any potential security problems. Users can then examine, query, and analyze the output with an HTML browser, such as Mosaic, Netscape, or Lynx. While the program is primarily geared towards analyzing the security implications of the results, a great deal of general network information can be gained when using the tool - network topology, network services running, types of hardware and software being used on the network, etc.

However, the real power of SATAN comes into play when used in exploratory mode. Based on the initial data collection and a user configurable ruleset, it will examine the avenues of trust and dependency and iterate further data collection runs over secondary hosts. This not only allows the user to analyze her or his own network or hosts, but also to examine the real implications inherent in network trust and services and help them make reasonably educated decisions about the security level of the systems involved. SATAN can be download here:

http://jackets.gt.ed.net/satan-1.1.1/docs/satan_overview.html

# CrackerJack -




# Password Cracking Programs

Password cracking programs are designed to break into various programs using a variety of methods. Some of these programs use dictionary attacks by systematically trying thousands of popular passwords such as spring, summer, baseball, 12/25/98, etc. These programs will also test to see if common default user name and passwords will work (such as ADMIN, PASSWORD). Other password cracking programs use brute force attacks where all possible combinations of letters and numbers are systematically checked against a logon screen.

Crackamibios 1.1
AMI Read the password
AMI bios for newer bios w/ source
Show BIOS password
Remove SETUP password
AMI-bios password viewer
ARJ password cracker from Russia
Break ZIP
Brute-force cracking
Find a zip password
PKzip archive cracker fast!
Password guesser for ZIP file
Crack ZipFile Passwords
Claymore for windows is a brute force cracker
CrackerMate is a game cracking program
Intruder 2.1 will remove ANY protection from BP/TP/BCPP/TC/MSC/CLIPPER program
Delam's Elite Password Leecher
Jill 2.0 Cracking utility for CrackerJack
Prepare lists for CrackerJack
Novell Password crack
Password breaker generic
Permut is a simple tool to generate passwords
POPcrack popmail password cracker
Trumpet Winsock Password Cracker
Automated Password Generator
RemoteAccess uerlist password hacker
Netware Password catcher
Therions Password Utility Word list manipulation tool
Unix password hacker
Microsoft Word Password cracker
Word for Windows Password cracker
crack WinCrypt files

## E-Mail Tools

Files related to causing destruction over e-mail (bombing) and recovery from said bombing.

**Anonymous Senders:**
Win95 Anonymail - Anonymous emailer
SendFake - Send e-mail from addresses of your choosing

**Bombers:**
Avalanche 3.6 - The newest version of a great bomber
CompuServe Based E-Mail Bomber - E-Mail bomber
Death 'n Destruction: 4.0 - E-Mail bomber - Includes tools to resolve IPs, send OOB packets, finger, and list on ports.
Extreme Mail Beta 1 - New Mail Bomber, Decent
Homicide - Good mail bomber
Kaboom v3 - An easy to use e-mail bomber - Includes mailing lists
Mail Bomber v .02b - Mail bomber
Mail Flash - Sends mail to screw over UNIX mail terminals
Nemesis Mail Bomber 1.0 - Anonymous bomber - Uses telnet.exe to send mail
QuickFrye - Bomber & Anonymous mailer
The Unabomber - Mail bomber with great anonymizing capability
Up Yours 4 Beta 3 - Bomber & Anonymous sender - Supports HELO spoofing

**Clean Up:**
BombSquad v2.0 - Clean up after you've been email bombed
Mail Check - Check servers for anonymous mail

## Flooder Tools

Flooders are programs designed to severely lag a person's connection, sometimes to the point of them being disconnected.

**ICMP Flooders:**
Technophoria Battle Pong - ICMP flooder
Kaput 1.0 beta 1.5 - ICMP and Finger flooder
Final Fortune 2.4 - ICMP clone flooder
Hak Tek Version 1.1 - ICMP Flooder, Mail bomber, Anti-bomber, Port scanner
ICMP Bomber! - ICMP flooder
ICMP Flooder v0.2 - ICMP flooder
IPing 32 - Ping Tool
IWD Simpe ICMP Bomber - ICMP flooder
Ping - ICMP tool/flooder - Comes with Windows 9x
Sonar v1.0.2 - ICMP tool
Trumpet Ping - ICMP flooder
Vai-te já ICMP ToolKit v2.01 (English Version) - ICMP Bomber, Nuker, Nuke Detector, and an OOB Attacker
Vai-te já ICMP ToolKit v2.01 (Portugese Version) - ICMP Bomber, Nuker, Nuke Detector, and an OOB Attacker
X-Script ICMP Bomber v0.3 By Code - ICMP flooder

**UDP Flooders:**
Pepsi - UDP flooder
UDP Port Nuke - UDP Flooder
UDP2 v10.2 - UDP Flooder
UDP Blaster v1.53 - UDP Flooder
UDP Flooder - UDP Flooder
surge UDP Port Flooder - UDP Flooder
Rebellion UDP Flooder - UDP Flooder
UDP PRO v2.0 - UDP Flooder
surge UDP Port Spammer - UDP Spammer
UDP Datastorm - UDP Flooder
Wpepsi - UDP flooder for DOS

**Port Bombers:**
Beer - Mass connection port flooder
Bmb2 - Mass data port flooder
Boom - Port bomber
Gewse97 - Mass data port flooder
Internet Packet Tools v1.00 Build 300 - Floods TCP or UDP Ports
Mutilate - Mass connection port flooder
Octopus - Mass connection port flooder
DOS Panther Modern Mode 1 - Port bomber for 56k connection
DOS Panther Modern Mode 2 - Port bomber for T3 connection
PortFuch 1.0b2 - Mass connection port flooder
Pounder Alpha 1 - Mass connection port flooder

## ICQ Tools

Programs designed to kill ICQ and people over ICQ. ICQ is an instant messaging, chat, and file transfer program by Mirabilis.

**Clean Up:**
ICQ DeFlooder v1.0 - Deletes all unread messages after a bomb
ICQ Bombsquad - Cleans up after receiving a bomb
ICQ SWAT - Deletes bomb messages

**ICQ Flooders:**
IcnewQ - Spoof messages, bomb, kill ICQ
ICQ Message Flooder - Sends large numbers of messages from spoofed UINs
ICQ Flooder '95 - Bombs target from random UINs
IcKiLLeR - Sends mass messages from random UINs
ICQZap - Message bomb from random UINs
ICQRevenge - Message bomber

**IP Sniffers:**
ICQ IP Address Unmasker - Shows IP despite hiding
ICQ IP Sniffer - Shows IPs of even hidden ICQ users

**Protection:**
Warforge ICQ Protect - Protects from ICQ Bombs
ICQ Bomb/Hacking Utility Protector - Opens 14 ports to confuse scanners
WarForge ICQBomb Protection System v2 - Protects ICQ from being bombed

**Miscellaneous:**
ICQ Auto Authorize - Adds anyone to your contact list without their permission
ICQ Port Sniff! - Finds the port that ICQ is running on
ICQ Source UIN Spoofer - Send anonymous ICQ messages

## IRC Tools

Internet Relay Chat tools are programs designed to generally knock people off IRC any way possible.

**Clone Flooders:**
Excess Flood 2.9 - Loads clones to flood users
Floodbots Flooder 2.0 - Clone flooder
Floodbot Front End v0.2 - Companion shell for Floodbots Flooder 2.0
iRC kiLLer pRO! - Combines Flash, Floods v2.4, Multi-CollideBot 95, and SUMO/95 v 1.1 Lag Killer!
SUMO/95 1.1 Lag Killer - Flooder
WaKo FloodBots 2.5 (7th Sphere) - Clone Flooder

**DCC Attacks:**
DCC Fuker 1.2 - DCC Flooders for mIRC
DCC Locker '97 - Can lock dcc chats in mIRC
DCC Unfer - Locks DCC Chats in mIRC

**Hanson Programs:**
Bug Exploit 1.5 - Attacks mIRC 5.3x
DeeP FreeZe II - Attacks mIRC 5.3x
DCC of Death - Kills mIRC 5.4
mIRC Freeze - Freezes mIRC
mIRC Slap - Attacks mIRC 5.3x

**ICMP Unreach Disconnectors:**
Click 1.4 - Uses the ICMP_Unreach bug to disconnect clients from IRC
Click 2.2 - New version for Winsock 2.2
Wnewk - Simple disconnector
Wnewk-X - Newer version of Wnewk
WNuke (WinNuke v1) - Unreach disconnector
WNuke ][ - Updated version
WNuke 4 - Newest version

**Link Lookers:**
Link Looker for Windows95 Ver 1.61 (GOLD BETA) - Looks for IRC Server Splits
Link Looker for Windows 95 Ver 2.2 - Looks for IRC Server Splits
xLinkLooker Version 1.0a - Looks for IRC Server Splits

**Miscellaneous:**
Lynch0 - Floods IRC servers with bogus server login attempts
Multi-CollideBot 95 - Collides nicknames off IRC

## Key Loggers

Programs to log all keystrokes on a computer to file. They are usually used to capture usernames and passwords.

IK
Key Log 2
Key Log '95

## Network Tools

Programs built to give you any information possible about a target address, or to help you find an address that has certain characteristics.

**Port Listeners:**
ICMP Monitor Version 0.92 - ICMP detector with a DNS lookup tool
ICMP Scan v2.0 - Scans for connected IPs
ICMP Datagram Sniffer v1.0 Alpha 5 - ICMP detector for DOS
ICMP Watch v1.3 - 7th Sphere - Detect incoming ICMPs
Nuke Nabber 2.9 - Listens on 50 chosen ports for TCP and UDP attack + ICMP_UNREACH
Nuke Detector v1.0 - Port 139 Nuke Detector
Nuke Nabber 2.5 - Catches & logs incoming nukes
The Port Block vo.o5b - Blocks chosen ports
Skream's Port Listener v2.3 - Listens on a chosen port
PortListener v2.2a - Listens on a chosen port
Port139 Watcher - Port 139 Nuke Detector
ninX's Port Blocker b100 - Blocks chosen ports
X-NetStat - Shows you your active internet connections

**Port Scanners:**
Cabral's Domain Scanner Final - Scans C block of addresses
Cha0scanner v2.0 - Port scanner
FTP-Scan - Anonymous port scanner, works through an FTP server
Host Scanner - Scans chosen domain for all host names
Mirror Universe 2.1 - Gives NetBios information about a target system
Netcop v1.6 - DNS Resolving, Domain WHOIS Data
NetGhost DomainScanner - Scans domain for a chosen port
Ogre - Checks servers for open FTP, HTTP, SMTP, Telnet, etc... & for misconfigurations
OstroNet - Whois client, Finger client, Port scanner, Domain Scanner
PortPro v0.93 - Port scanner that can flood open ports
PortSage - Port scanner
Rebellion v2.0 portscanner - Port scanner
Port Surveillance v.05 - Scans a port
Port Scanner 1.1 - Scans a group of IP addresses looking for certain open ports
SiteScan - Scans for exploits: PHP, Finger Flaws, PHF, Handler, _vti_pvt, Service.pwd, IISAdmin, Wrap, aglimpse, test.cgi, *.pwl, *.pwd

## Nuker Tools

Programs that exploit the Out of Band Data and Invalid Fragmentation bugs in Windows and some UN*X variants. These programs do everything from killing the TCP/IP subsystem until the next restart to disable your operating system.

BitchSlap v1.0 - Port 139 OOB Nuker
Blood Lust - Chosen Port OOB Nuker
BlueRain's Port 139 OOB Attack Prog Version 1.0 - Chosen Port OOB Nuker
CGSi OOB Message GFP Gen - Chosen Port, Multi-IP OOB Nuker
DIE - Port 139 OOB Nuker
DIE3 - Chosen Port OOB Nuker
DIE3NT - Kills Windows NT Running DNS on Port 53
Divine ]I[ntervention 3 - OOB Attack, ICMPer, Icq Killer, Mail Bomber, Mass Subscriber, DCC Flood Bot, and Text Flood Bot
Death 'n Destruction: DoS - OOB Attack, Port protector
Calvin's Labs NetAttact - Chosen Port, Size and Number OOB Nuker
F-ed Up 2.0 - Chosen Port OOB Nuker
KiLLmE v1.0 - Port 139 OOB Nuker
KillWin - Chosen Port and Number OOB Nuker
Knewk'em All v1.0 - Chosen Port and Number OOB Nuker
Meliksah Nuker v1.0 - Chosen Port and Number OOB Nuker
MS Nuke - Port 139 OOB Nuker

Muerte - The first, best, and only OOB exploit you will ever need - IP, Port scanning
Nuke v 2.3 - OOB Attack, death confirm
Nuke Attack - Chosen Port OOB Nuker
Nuker 1.02 Beta - Port 139 OOB Nuker
WinNUKE - Port 139 OOB Nuker
WinNuker v0.2 - Multi-Port OOB Nuker
WinNuke V95 - Port 139 OOB Nuker
WNUKE32 (Build 69) - Port 139 OOB Nuker
WinNuke for Win95 v1.1 - OOB to port 135 or 139 - Includes patch

## Spoofing Tools

Programs to make you look like you're coming from some other address on the Internet (mostly used on IRC)

**IdentD Spoofers (Identity Spoofers):**
DC Internet Services
EyeDent
WinSpoof '97

**DNS Spoofers:**
cha0s IP Spoofer - Cache a "ghost connection" on an IRC server
Erect '97 - DOS port of "erect" spoofer, requires access to name server
Jizz - DOS port of "jizz" spoofer, requires access to name server
Spewfy - Cache a "ghost connection" on an IRC server

## WinGate Tools

WinGate is a program that allows a computer to act as a gateway between networks. These programs exploit WinGate.
wGateScan v2.2 - Scans B and C blocks for active WinGates
zFn - Loads IRC flood clones through WinGate

## Phreaking Tools

beige box Instructions for making a linemans handset.
blue box Generates 2600 Mhz tones.
chartreuse box Lets you take power from a phoneline.
chrome box Allows manipulation of traffic lights.
crimson box Lets you put people on hold.
gold box I'm not sure what this is for.
neon box Good for recording tones, or anything else
white box Change a normal touchtone keypad into a portable unit

## Cracking & Hacking Newsgroups:

alt.cracks - Great Place to get Cracks.
alt.cracker - Cracks Forum, get and request Cracks.
alt.hackers - Hackers Forum.
alt.hackintosh - Forum on Hacking Macintosh.
alt.hackers.malicious - Malicious Hackers Forum.
alt.binaries.warez.ibm-pc - Get some WareZ.
alt.binaries.warez.ibm-pc.d - Get some WareZ.
alt.binaries.warez.ibm-pc.gamez - Get some Gaming WareZ.
alt.binaries.warez.ibm-pc.old - Get some Older WareZ.

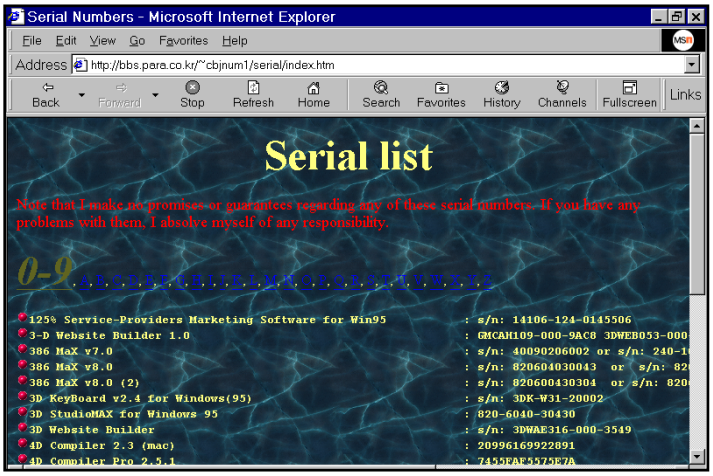
## Key Generators & Registration Tools

AbsoluteFTP v1.0b9 - Time/Nag crack
ACDSee32 2.x - Key generator
Age Of Empires - Microsoft Age Of Empires 1.0a update crack
Age Of Empires - Microsoft Age Of Empires CD crack
Agent 0.99x - Serial# generator for Agent 0.99e - k
Agent 1.5 - Agent 1.5 build 452 x-header patch
Agent 1.x - Serial# generator for Agent 1.x
Andretti 98 - Andretti 98 - Crack Patch
Bryce 2 - Bryce 2 demo Update
Catz 1.00k - Catz Demo 1.00k Crack
CD Quick 3 - Key Generator
CD/Spectrum pro 3.2.327 - CD/Spectrum Pro Version : 3.2.327 Patch
CDDA 1.7 - CDDA (DA2WAV) 1.7 keyfile maker
CleanSweep 3.0 Trial - CleanSweep 3.0 Trial crack patch
Clock Manager - Key Generator
ComSpy win98/95 - Keyfile maker
Cool Edit 96 - Cooledit v.1.52 - Key Generator
CuteFTP32 - Hidden Files & Folders Patch
CuteFTP32 v1.7/1.8 - Keyfile builder for CuteFTP
CuteFTP32 v2.0 - CuteFTP 2.0 FINAL keyfile creator
Dark Reign - CD-ROM check crack
Dark Reign - Dark Reign CD check crack
Dogz - ADOPTDOG .03 - Registration Generator for DOGZ
Dogz v1.8Q - DOGZ v1.8Q REgistration Crackz
Ecopad32 v3.31 - Key Generator
Email Address Sniffer 2.1 - Patch
Eudora - Eudora X-Header editor
Eudora Pro 4 - Demo expiration patch
F-22 Lightning II - F-22 Lightning II crack
GameSpy 1.01 - GameSpy 1.01 registration patch
GameSpy 1.50 - GameSpy 1.50 FINAL registration patch
GameSpy 1.52 - GameSpy 1.52 key generator
GameSpy 1.52 - GameSpy 1.52 regpatch
Gear Replicator 1.2 - Unlock Generator
Ghost - GHOST v2.1.4 "KEYMAKER"[JAM/UCF]
GIF Construction Kit - GIF CONSTRUCTION SET *KEYMAKER*
Graphics Workshop - Brute force reg hacker
Graphics Workshop 95 - Key Generator
Hard Disk Sleeper 1.4 - Key Generator
Hexen 2 - Hexen 2 CD crack
HomeSite v2.0 - HomeSite v2.0 Key Generator
HomeSite v3.0 - HomeSite v3.0 patch
HotDog Pro 4.5+ - Key Generator
HotDog32 1.0 - CRACK-PATCH
HyperSnap 2.64 - Key Generator
ImageView 95 1.2 - Key Generator
Internet Conference Professional 1.2 - Key Generator
Internet Phone v4.5.03 - Internet Phone v4.5.0.3 crack

Internet Phone v4+ - Internet Phone v4+ [CraCk PatCh]
Internet Phone v5.0 - Internet Phone v5.0 build 114 patch
Internet Phone v5.0 - Internet Phone v5.0 build 135 patch
Kaleidoscope 95 - Key Generator
Live Image 1.26 - crack patch
LView Pro - Key Generator
LView Pro 95 - Key Generator
Magic Folders 97.10a - Key-file
Magic Notes 1.6 - Key Generator
MDaemon - Registration Code Generator
Microangelo - Microangelo 95 v2.x *Keymaker*
Microsoft - MS-Code Generator 1.01 (all products)
Microsoft Freecell - Undo enabler patch
Microsoft Project 98 (8.0) - Evaluation Patch
mIRC 5.3 - key generator
mIRC V4.52+ - mIRC V4.52+ *kEYMAKER*
mIRC V5.00+ - Keymaker for mIRC 5.00 onwards.
MOD4Win 2.30 - Mod4Win 2.30+ KeyMaker Patch
Money 98 - MS Money 98 (6.0) crack patch
Moto Racer - MoToRaCeR *uNiVeRSaL CRaCK*
Nearside - Build 554 Regpatch
Netbar 2.0 - Key Generator
NetTerm 2.8.9 - Key Generator
NetTools - Key Generator
Norton AntiVirus 2.01 Trial - Crack Patch
NTcrt 1.0B6 - Key Generator
Office 97 - Microsoft Key Generator 2.0
Paint Shop Pro 4.14 - Shareware crack
Personal Stock Monitor 1.1 - Key Generator
PGP Manager32 1.6b - Key Generator
PKZIP - Authenticity Verification
Power Desk - kEY mAKER
Pretty Good Solitaire 3.97.2 - Key Generator
Quake 2 - Quake2 v3.09 Update CD check removal
Quake 2 - Quake2 v3.10 Update CD check removal
RAS+ 95 - Key Generator
SciTech Display Doctor 5.2 - uNIVBE v5.2 *kEY-mAKER*
SciTech Display Doctor 6.0 - Key Generator
SciTech Display Doctor 6.0 - Retail Key Generator
SciTech Display Doctor 6.0 - Trial Patch
Secret Agent 1.12 - Key Generator
Serv-U FTP - sERV-u 2.xX *kEYMAKER*
SideKick 98 - Unlock code generator
Snapshot/32 2.55 - Key Generator
Sound Gadget Pro - Key Generator
Stiletto 96a - Key Generator
Sub Sink Pro 97 - Key Generator
Thumb Plus 2.0 - Key Generator
Thumbs+Plus v3.0c - Patch
ThumbsPlus32 v3.10 - Time Limit/Nag Screen Crack
Trumpet WinSock 95 - Key Generator
Uedit32 4.0 - Key Generator
UNIVBE 5.x - uNIVBE v5.2 *kEY-mAKER*
Virtual CD-ROM - Unlock Code Generator
Visual Basic 5.0 - Microsoft Key Generator 2.0
Visual C++ 5.0 - Microsoft Key Generator 2.0
Visual C++ 5.0 - Microsoft Key Generator 2.0
WebImage 95 - Key Generator
WinArj 95 - reg code generator
WinArj 95 - WinArj95 v4.1.0x crack
Windows 95 - MS-Code Generator 1.01 (all products)
Windows Commander v3.0 - Windows Commander 32bit CRACK
Windows NT 4.0 - Microsoft Key Generator 2.0
Windows NT 4.0 120 day trial - NT 4.0 Server 120 Day Demo Crack Kit
WinGate 1.x - Key Generator for v.1.3.08 onwards
WinGate 2.0 - Key Generator for Pro and Lite
Winimage 2.25 - Key Generator
WinPack 32d - Key Generator
WinPGP 4.0 - Key Generator
WinPlay3 v2.0 - NOT A CRACK! - Patch to turn panel green
WinPlay3 v2.0 - WiNPLaY 3 VeRSioN 2.0 crack
WinRar 2.00 - WinRAR 2.00b - Key Generator
WinZip - WinZip Reg-Number Generator
WinZip Self-Extractor - WinZipSelfExtract Reg Key Maker
Wipeout XL - Crack
WS Ftp Pro 4.50 - Crack to remove the expiration
Xara3D 1.05 - Crack Patch
Xing MPEG Encoder v2.0 - key maker
XWing vs Tie - Crack patches for 1.1 & 3D updates

# Serial Lists

Serial Lists are rampant on the Internet. These sites contain known access codes that allow you to install and use virtually any software applications you could name today. The distribution of these access codes are of course illegal, and therefore none of these illegal codes are




# Other Tools

**Ping** - (Packet Internet Groper) a basic Internet program that lets you verify that a particular Internet (IP) address exists and can accept requests. The verb *ping* means the act of using the ping utility or command. Ping is used diagnostically to ensure that a user's PC is properly connected to the Internet. If, for example, a user can't ping a host, then the user will be unable to use a browser or any other TCP/IP application with that host. Ping can also be used to learn the number form of the IP address from the symbolic domain name.

**Sniffer** - A sniffer is a program that monitors and analyzes network traffic, detecting bottlenecks and problems. Using this information, a network manager can keep traffic flowing efficiently. A sniffer can also be used illegitimately to capture data being transmitted on a network. A network router reads every packet of data passed to it, determining whether it is intended for a destination within the router's own network or whether it should be passed further along the Internet. A router with a sniffer, however, may be able to read the data in the packet as well as the source and destination addresses.

**Spoof** - 1) To deceive for the purpose of gaining access to someone else's resources (for example, to fake an Internet address so that one looks like a certain kind of Internet user) 2) To simulate a communications protocol by a program that is interjected into a normal sequence of processes for the purpose of adding some useful function

**Warez** - (pronounced as though spelled "wares" or possibly by some pronounced like the city of "Juarez") is a term used by software "pirates" to describe software that has been stripped of its copy-protection and made available on the Internet for downloading. People who create warez sites sometimes call them "warez sitez" and use "z" in other pluralizations.

**Exploits** - an Exploit is a program that 'exploits' a bug in a specific software. All exploits are different, they do different things and exploit different bugs, that's why exploits are always program specific. Exploits are made to get root on different operating systems. They achieve this by exploiting a bug in software when the software is running as root. In UNIX type OS's, software may have to run as root (or UID 0) in order to perform a specific task that cannot be performed as another user. So basically the exploit crashes the software while running as root to give you the beautiful root prompt.

# Pirated Software

## Chapter 38

## Are You at Risk?

Has your company illegally installed multiple copies of a software program on multiple computers? Is your company using pirated software? If so, you are at risk. If you are caught, the penalties can be huge. For example, one Louisiana hospital was found to be running 500 copies of WordPerfect, and copied from a single copy of WordPerfect which itself was pirated. The company was caught and fined more than 2.5 million dollars.

## Penalties for Using Pirated Software

Illegal distribution of software can subject a seller to arrest and felony charges with fines up to US$250,000 and prison terms of up to 5 years. If the copyright owner brings a civil action against you, the owner can seek to stop you from using its software immediately and can also request monetary damages. The copyright owner may then choose between actual damages, which includes the amount it has lost because of your infringement as well as any profits attributable to the infringement and statutory damages, which can be as much as $150,000 for each program copied.

## Who is Responsible?

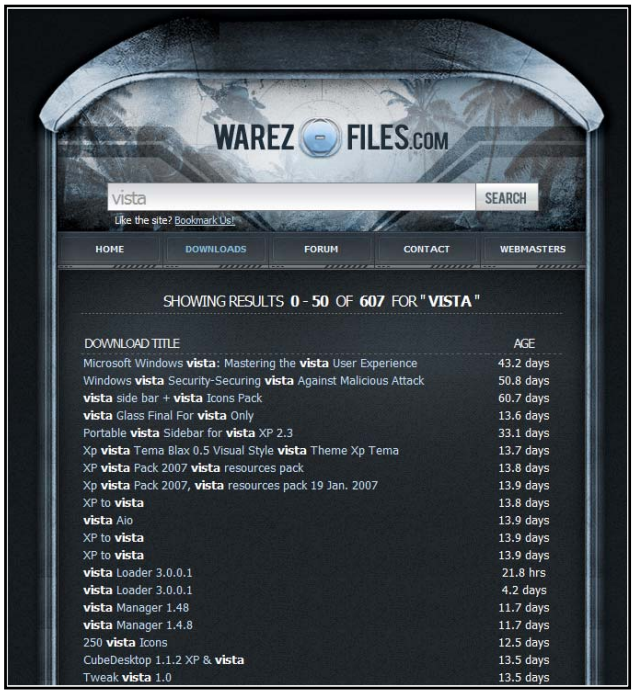
Company officials can be held responsible if they know about the use of pirated software, or if they take no measures to track and deter the use of pirated software. Simply looking the other way is not good enough in some states and jurisdictions. Under "vicarious liability" of the US Copyright Act, an employer is liable for acts committed by its employees when those acts are within the scope of their employment duties. Another theory of liability is the doctrine of contributory copyright infringement, whereby a party who does not do an infringing act but who aids or encourages it is liable for the infringement.

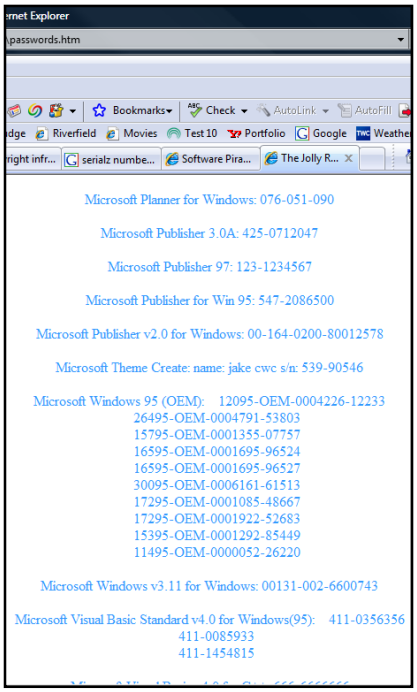
## Sources for Pirated Software

1. **Illegal Copies -** Legitimate software copied illegally on additional computers becomes pirated software. Most license agreements allow the same user to install software on both their laptop and desktop computers, provided they use only one copy of the software at a time.

2. **The Black Market -** The streets of Hong Kong are full of pirated software – products that sell for hundreds of dollars in the US are widely available for $5.00 on the black market.


3. **WAREZ & SERIALZ** – (Pronounced "wears", this term is hacker slang for "illegal software"). Tens of thousands web sites exist where you can download virtually any software on the planet. Once downloaded, thousands more SERIALZ (pronounced "cereals", this term is hacker slang for "illegal serial numbers") provide serial numbers that you can (attempt) to use in order to install the product.



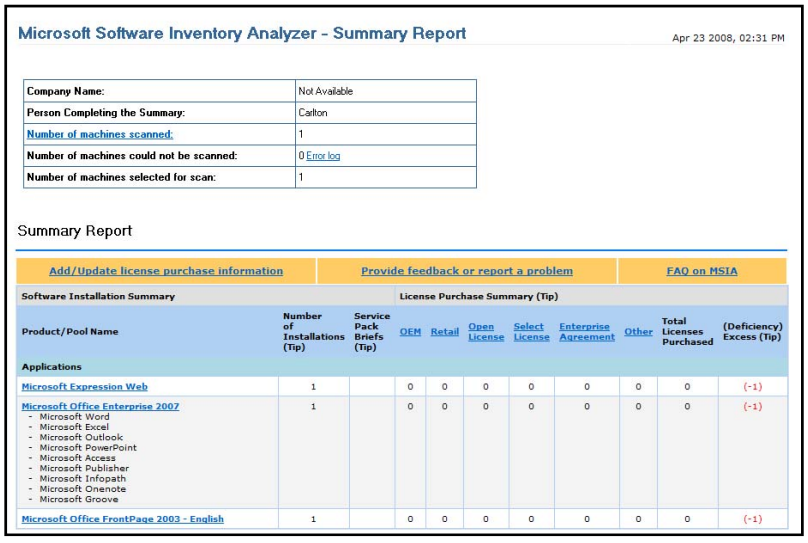



4. **Counterfeit Software -** Yes, counterfeiters have gotten that good, and some counterfeit software finds its way into the main stream. The industry is finding ways to fight back (such as the edge-to-edge holograms for Office XP, Windows 2000 and Windows XP CD-ROMs).

## How to Find Pirated Software in Your Organization

Both Microsoft and the Business Software Alliance provide software management guides and tools that can help you organize and maintain your software inventory. You will get a better handle on what you need to purchase and what you need to eliminate to become compliant. These resources will help you determine if you have purchased genuine or counterfeit software.

As an example, the Microsoft® Software Inventory Analyzer tool generates an inventory of the core Microsoft products installed on your local computer, or throughout a network. The MSIA is built specifically to be a starting point to working with Microsoft's Software Asset Management (SAM) tools, and to that end, it will work with networks that have 250 computers or less; and will locate only Microsoft software. The results of the scan performed by MSIA are confidential they are not sent to Microsoft. A sample report is shown below.



Microsoft Software Inventory Analyzer - Summary Report

Apr 23 2008, 02:31 PM

| | |
|---|---|
| Company Name: | Not Available |
| Person Completing the Summary: | Carlton |
| Number of machines scanned: | 1 |
| Number of machines could not be scanned: | 0 Error log |
| Number of machines selected for scan: | 1 |

Summary Report

Add/Update license purchase information | Provide feedback or report a problem | FAQ on MSIA

| Software Installation Summary | | | License Purchase Summary (Tip) | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Product/Pool Name | Number of Installations (Tip) | Service Pack Briefs (Tip) | OEM | Retail | Open License | Select License | Enterprise Agreement | Other | Total Licenses Purchased | (Deficiency) Excess (Tip) |
| Applications | | | | | | | | | | |
| Microsoft Expression Web | 1 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | (-1) |
| Microsoft Office Enterprise 2007<br>- Microsoft Word<br>- Microsoft Excel<br>- Microsoft Outlook<br>- Microsoft PowerPoint<br>- Microsoft Access<br>- Microsoft Publisher<br>- Microsoft Infopath<br>- Microsoft Onenote<br>- Microsoft Groove | 1 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | (-1) |
| Microsoft Office FrontPage 2003 - English | 1 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | (-1) |

You should update and clean up your software inventory at least once a year. Whether you outsource the job to a reseller or IT specialist, or do it in-house, make reviewing your inventory an annual event. Purchase the software and sign up for the licenses you really need, and comply with the terms. Get rid of the rest.

http://www.microsoft.com/resources/sam/msia.mspx?lm=

# 15 Top Security / Hacking Tools & Utilities

## Chapter 39

**1. Nmap -** Nmap ("Network Mapper") is a free open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers and both console and graphical versions are available. Nmap is free and open source.

Can be used by beginners (-sT) or by pros alike (–packet_trace). A very versatile tool, once you fully understand the results.

**2. Nessus Remote Security Scanner -** Recently went closed source, but is still essentially free. Works with a client-server framework. Nessus is the world's most popular vulnerability scanner used in over 75,000 organizations world-wide. Many of the world's largest organizations are realizing significant cost savings by using Nessus to audit business-critical enterprise devices and applications.

**3. John the Ripper - JTR 1.7 was recently released**! John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), DOS, Win32, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP/2003 LM hashes, plus several more with contributed patches.

**4. Nikto -** Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 3200 potentially dangerous files/CGIs, versions on over 625 servers, and version specific problems on over 230 servers. Scan items and plugins are frequently updated and can be automatically updated (if desired).

Nikto is a good CGI scanner, there are some other tools that go well with Nikto (focus on http fingerprinting or Google hacking/info gathering etc, another article for just those).

**5. SuperScan -** Powerful TCP port scanner, pinger, resolver. SuperScan 4 is an update of the highly popular Windows port scanning tool, SuperScan.

If you need an alternative for nmap on Windows with a decent interface, I suggest you check this out, it's pretty nice.

**6. p0f -** P0f v2 is a versatile passive OS fingerprinting tool. P0f can identify the operating system on:

- machines that connect to your box (SYN mode),
- machines you connect to (SYN+ACK mode),
- machine you cannot connect to (RST+ mode),
- machines whose communications you can observe.

Basically it can fingerprint anything, just by listening, it doesn't make **ANY** active connections to the target machine.

**7. Wireshark (Formely Ethereal) -** Wireshark is a GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames. The goal of the project is to create a commercial-quality analyzer for Unix and to give Wireshark features that are missing from closed-source sniffers. Works great on both Linux and Windows (with a GUI), easy to use and can reconstruct TCP/IP Streams! Will do a tutorial on Wireshark later.

**8. Yersinia -** Yersinia is a network tool designed to take advantage of some weakeness in different Layer 2 protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems. Currently, the following network protocols are implemented: Spanning Tree Protocol (STP), Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), Dynamic Host Configuration Protocol (DHCP), Hot Standby Router Protocol (HSRP), IEEE 802.1q, Inter-Switch Link Protocol (ISL), VLAN Trunking Protocol (VTP).

The best Layer 2 kit there is.

**9. Eraser -** Eraser is an advanced security tool (for *Windows*), which allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns. Works with Windows 95, 98, ME, NT, 2000, XP and DOS. Eraser is Free software and its source code is released under GNU General Public License.

An excellent tool for keeping your data really safe, if you've deleted it..make sure it's really gone, you don't want it hanging around to bite you in the ass.

**10. PuTTY -** PuTTY is a free implementation of Telnet and SSH for Win32 and Unix platforms, along with an xterm terminal emulator. A must have for any h4×0r wanting to telnet or SSH from Windows without having to use the crappy default MS command line clients.

**11. LCP**

Main purpose of LCP program is user account passwords auditing and recovery in Windows NT/2000/XP/2003. Accounts information import, Passwords recovery, Brute force session distribution, Hashes computing.

A good free alternative to L0phtcrack.

LCP was briefly mentioned in our well read **Rainbow Tables and RainbowCrack** article.

**12. Cain and Abel –** Most hacker's favorite for password cracking of any kind.

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing

routing protocols. The program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort.

**13. Kismet -** Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic.

A good wireless tool as long as your card supports rfmon (look for an orinocco gold).

**14. NetStumbler -** Yes a decent wireless tool for Windows! Sadly not as powerful as it's Linux counterparts, but it's easy to use and has a nice interface, good for the basics of war-driving. NetStumbler is a tool for Windows that allows you to detect Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g. It has many uses:

- Verify that your network is set up the way you intended.
- Find locations with poor coverage in your WLAN.
- Detect other networks that may be causing interference on your network.
- Detect unauthorized "rogue" access points in your workplace.
- Help aim directional antennas for long-haul WLAN links.
- Use it recreationally for WarDriving.

**15. hping -** To finish off, something a little more advanced if you want to test your TCP/IP packet monkey skills.

hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.

# Safety Online

## Chapter 40

## Safety Online

Using the internet and surfing the web can be as sweet and easy. Unfortunately at other times, online surfing can put you at risk. This chapter discusses a few common sense recommendations to help you stay safe during your online activities.

1. **No Personal Information** - Do not give out your personal information (full name, address, or phone number) to anyone online that you don't know or trust because they might not be who they claim to be.

2. **Verify That Friends Are Who They Say They Are** - To avoid confusing your friends with strangers online, consider using a password or code word. Or you could simply call your friend to make sure they are online.

3. **Financial Data –** Only give out your bank account or credit card information to web sites you trust, and make sure that they are using encryption (ie: the gold lock and https:// is used to indicate that the web site is secure.

4. **Never Open E-Mail Attachments -** Never open e-mail attachments from strangers unless you can trust them and you have security settings on your computer. Unknown e-mails may contain viruses or spyware that can harm your computer.

5. **Beware Of Spoof Email -** Beware of spoof email claiming to be from eBay, PayPal, or a bank or a company name you know asking for personal or sensitive information. This is called *phishing*. The e-mail may inform you that there is a problem with your account/password. There may be a link to click inside, or even a phone number to call.

6. **Online Arranged Meetings -** If you decide to meet someone in person from online, go to a public place and let friends and family know your plans. Have an alternate plan if things turn out badly.

7. **Anti-Virus Software -** Get a good anti-virus program, spyware remover, and firewall. There are free programs available online, such as Avast! antivirus, Grisoft's AVG Free, Microsoft Anti-Spyware and Spybot, and Sygate personal firewall. They will block most attempts and alert you if problems are found.

8. **Read The Fine Print -** There are many survey sites that pay you for answering questions and filling out forms. If you do not want to receive junk mail or get put on a telemarketer list, look for a small box near the bottom of the page that asks if you want to receive information and offers from other companies. The best sites will have a statement listed that they will not sell your name to other companies. Some sites require you to give all your information to get the product. Although sometimes, you may get a ton of spam. Only fill in required

fields that are marked with a *. If the info box does not have an asterisk, it is optional and you can leave it blank.

9. **Monitor Children -** Monitor young children's (under 16) activities closely and use parental controls when available. Use a password a child will not guess. Install parental control software. The Internet is not child-friendly.

10. **Use Strong Passwords** – As discussed in the Use strong passwords Chapter.

11. **Limit Your Buddy List** - Web services such as SYPE, AOL, Yahoo, or MSN have messengers that allow you to chat with others with an instant message (IM) or private message (PM) box. Go to the preferences or options menu and carefully choose settings. It is best to turn off messages from all users and only add people to your buddy list that you know very well or someone you choose to talk to.

12. **Use Add-on Messaging Programs** - YTunnelPro and YahElite are very good and helpful companions to Yahoo Messenger, and similar solutions are available for other messaging services.

13. **Subscribe To Unimportant Things With A Secondary E-Mail Address** - This will help keep you from getting spam to your regular address, and will protect your identity. A good site which allows you to create temporary email addresses on the fly is Spam Motel. When you register on an unknown site, go to Spam Motel and create an email address and delete it when you have no further use for it.


Gmail and Hotmail also offer free e-mail addresses that work good in temporary or less important purposes.

14. **Prepaid Credit Cards -** If you feel uncomfortable giving away your credit card number online, consider using a prepaid credit card or use a gift credit card instead. These often work the same as a regular credit card, but they only have a set amount on them, so that if someone gets a hold of the prepaid card's number, they don't do as much damage.

15. **WOT & NoSCRIPT -** If you`re using firefox, download the extensions WOT, which tells you how trustworthy sites are, and NoScript, which denies Javascript and other potentially malicious add-ons except on trusted sites.

16. **Watch Your Mouth -** Be careful what you say on the internet and understand that it is becoming common practice for employers to research what you have said online as part of the hiring process. What you say today could keep you from getting hired to your dream job five years from now.

17. **No Birthdates Online** - If you mention that you had a birthday recently, don't be specific about the date, or your exact age. These two items are enough to figure out your date of birth, a piece of info the banks use to help identify you.

18. **Watch the Downloads -** Be careful of what you download. If it's not open source/GNU, then make sure it's from a reputable site (widgets.yahoo.com, cNet's Download.com, etc.)*. When using P2P software such as Limewire, only download music and age appropriate video. Anything else could be filled with viruses and who knows what.

19. **Clear Your Browser's Cache Periodically -** The cache stores web pages, images, and even some information about you on your computer, and should be cleared from time to time.

20. **Block Cookies –** Disable cookies permanently, or from time to time if you are surfing questionable web sites. For example, when researching this security course, I turned off my cookies often as I accessed web sites that I was not sure of.

21. **Check to see if Your Computer Has Been Tracked -** There is no surefire way to know if your computer is being hacked; however, there are many ways to distinctly reduce the chances of it being compromised as follows:

22. **Install a Firewall Device** - Install a firewall as discussed in the Firewall Chapter of these materials. (Especially if connected to broadband via network card, consider installing a router between the DSL or Cable modem and the computer's network interface. This will move the public IP address from the computer to the router. The computer will receive a private IP address (provided by the router) and cannot be detected by hackers casually probing.

23. **Use Anti-Spam Software** - Turn on Junk Mail Filtering in Outlook or use Spybot or another similar tool.

24. **Remove Anti-Virus Software That You Are Unhappy With -** Disconnect your computer from the Internet when downloads are finished, as it will be vulnerable while we do this next step. Go into control panel, and choose add/remove hardware. Uninstall any poorly performing antivirus software you have currently installed. Install a new antivirus solution. Connect your computer to the Internet again, and allow them to update fully.

25. **Install KeyScrambler -** Consider installing KeyScrambler Personal add-on for FireFox. This add-on encrypts your keystrokes to protect your login information from key logging programs. If a hacker has a program inside your computer logging all your keystrokes to steal your passwords, all they will get from password fields on web pages is scrambled garbage.

26. **Install HijackThis -** If you want extra security from hackers install HijackThis – a tool that is designed as extra security against homepage hijacking

27. **Install Comodo BOclean** – This is a real-time antimalware scanner which works at registry level to stop malware installs.

28. **Update your Antivirus Software** - Verify that your Anti-Virus software is up-to-date at least once a week if it is the automatically updating type. Check daily if it must be manually updated. Windows will allow a great deal of time to elapse before alerting you that it is out-of-date. Most reputable anti-virus developers release updates every couple of days; more often than that if warranted. It's a false sense of security running a computer with out-of-date anti-virus definition files.

29. **ActiveX** - Don't install activeX controls from a website you don't trust.

30. **Be Suspicious of Thumbdrives** - Don't run applications or copy content from disks, thumbdrives, CDs, etc. that have been provided by others (including friends); or belong to you if they have previously been connected to another computer, *unless scanned with your anti-virus program first*. If an infected computer has accessed the data on the media, the data is likely to be infected as well.

31. **Be Suspicious of Web Sites** - Watch out for any websites requesting personal information. Unless you trust the site, it is unwise to give out your email, address, phone number, or even name.

32. **Beware Of Sights With Pop-Ups** - Typically they'll be putting other things on your computer.

33. **Block Pop Ups** - Use the Block Pop up settings or Install pop-up deleting software.

34. **Browse The Internet Using Proxies -** This will get rid of those nasty scripts that people use to identify your IP address among other things. It doesn't matter whether you use a CGI, PHP,

or anonymous proxy, they all have about even advantages and disadvantages. A good CGI/PHP proxy is Anonymouse. Also Proxy.org has a long list of this kind of proxy, which can be useful.

35. **Prevent Peeping -** It is extremely unlikely someone is watching you through a physical camera, binoculars, (or worse; a sniper scope) or screen recording device, but just to be on the safe side you might want to follow the some of these obvious steps:

    a. Close all blinds and drapes through which someone could watch your computer monitor.

    b. Don't let anyone you wouldn't trust with your life near your computer unsupervised.

    c. Look for anything unfamiliar that is plugged into your computer.

    d. Buy one of these or use the equivalent of a small red eyepiece surrounded by red LEDs, and scan the area around your computer.

36. **Always Assume That Your Online Activity Is Being Monitored -** If you are using the internet on a network that isn't private (such as at work, school, a library, or cybercafe), you are almost certainly being monitored. Don't do anything you wouldn't want the administrator(s) of that network seeing.

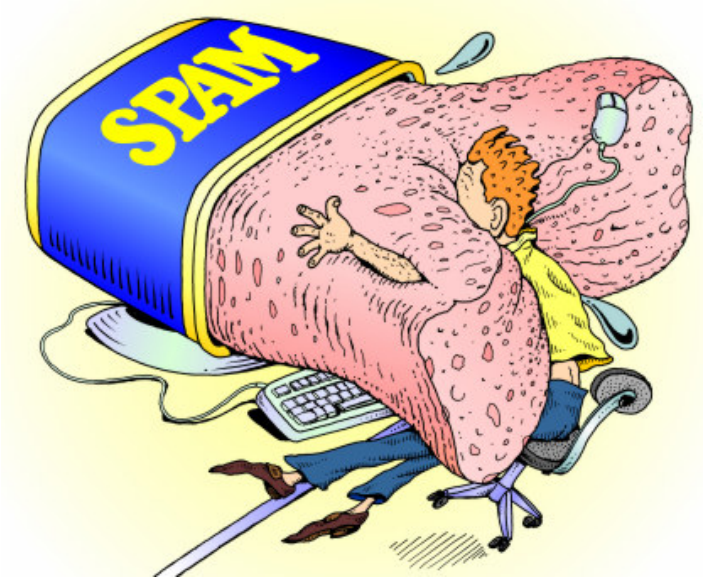
37. **Avoid Clicking on Advertisements -** Never click on an advertisement that isn't Google Adsense, and many times not even those. Doing so is a good way to get spyware and viruses on your computer.

38. **Encrypt Wireless Connections -** If you are using a wireless network to connect to the internet, encrypt it as strongly as you can. 32-bit is OK, 64-bit is good, 128-bit is better, and I sincerely doubt that you'll have access to 256-bit encryption, but if you do, I would use it.

39. **Secure your Passwords -** Keep your passwords secure.

40. **Never Remember Passwords -** Never let your browser remember your passwords. Likewise, don't tell sites to remember you. Some forms of spyware can read cookies that sites will give you when they store your passwords.

41. **Keep Ports Closed** - Don't open ports in your firewall or use UPNP. Crackers have found ways to break through your firewall using open ports, allowing them to monitor your computer.




# Blocking Spam

## Chapter 41

# SPAM

The word SPAM was originally created by Hormel Foods, maker of the canned "Shoulder Pork and hAM. Later Monty Python's Flying Circus performed a spam skit in which a restaurant serves its food with loads of spam, and the waitress repeats the word several times in describing how much spam is in the items. When she does this, a group of Vikings in the corner start a song: *"Spam, spam, spam, spam, spam, spam, spam, spam, lovely spam! Wonderful spam!"* Thus the meaning of the term is at least *"something that keeps repeating and repeating to great annoyance".*[(1)]

**How Big is the Spam Problem? -** The California legislature found that spam cost United States organizations alone more than $13 billion in 2007, including lost productivity and the additional equipment, software, and manpower needed to combat the problem. Ferris Research estimates the 2007 cost of Spam at $100 billion world-wide, and $35 billion in the US – more than double the cost in 2005. Presented below are a few statistics:

## Spam Statistics

| | Non Spam | Spam |
|---|---|---|
| 1. Total E-mails sent in 2006 | 6 Trillion (25 billion per day) | 18 trillion (75 billion per day) |
| 2. Average number of E-mails sent and received by each business user in 2006 | 600 per week | 1,800 per week |

3. The vast majority of spam messages are around 5KB.
4. Around 10% of spam messages are in the 100K-1MB range.
5. Around 5% of spam messages are bigger than 1MB.
6. Cost of a user deleting a spam message: $0.04
7. Cost of a user retrieving a bona fide message erroneously deleted as spam ("false positive"): $3.50

***Business Email Users, 2005-2010***

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|
| **North America** | 125.2 | 128.7 | 132.4 | 136.0 | 139.8 | 143.6 |
| **Europe** | 162.6 | 179.8 | 196.5 | 212.8 | 228.6 | 244.1 |
| **Other Americas** | 179.1 | 191.9 | 204.7 | 217.4 | 230.2 | 243.0 |
| **Africa** | 16.0 | 19.5 | 23.0 | 26.6 | 30.1 | 33.7 |
| **Asia (incl. Mid-East)** | 182.8 | 198.3 | 213.6 | 229.0 | 244.3 | 259.6 |
| **Oceania** | 8.7 | 9.1 | 9.5 | 9.9 | 10.4 | 10.8 |
| **Total** | 674.2 | 727.3 | 779.7 | 831.7 | 883.3 | 934.8 |

*Source: Ferris Research, The Email Security Market, 2005-2010*

Figures are in millions of users, rounded to the nearest 100,000.

## Where You Might Encounter Spam

1. E-mail Spam – Unsolicited e-mail, usually promotional.
2. Instant Messaging– Unsolicited chats sent to AOL, ICQ or Windows Live.
3. Chat Rooms – Online web sites where users communicate in real time.
4. Newsgroups and Forums – Web sites where users post comments.
5. Mobile Phone – Spam text messages sent to your mobile phone number.
6. Online Game Messaging – Messaging between gamers.
7. Search Engines (Spamdexing) – HTML code makes a page rank higher than it should.
8. Blog, Wiki, and Guest books – Spam takes advantage of open nature of comment pages.
9. Video Web Sites (like YouTube) – Spam usually appears in comments section.

## Spam Laws


In 2004, the United States passed the CAN-SPAM Act of 2003 which provided ISPs with tools to combat spam. For example, this act allowed Yahoo! to successfully sue Eric Head - reportedly one of the biggest spammers in the world. The law's primary provisions are as follows:

1. Bans false or misleading header information. Your email's "From," "To," and routing information – including the originating domain name and email address – must be accurate and identify the person who initiated the email.
2. Prohibits deceptive subject lines. The subject line cannot mislead the recipient about the contents or subject matter of the message.
3. Requires that your email give recipients an opt-out method.
4. Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your commercial email.
5. It's illegal for you to sell or transfer the email addresses of people who choose not to receive your email, even in the form of a mailing list, unless you transfer the addresses so another entity can comply with the law.
6. Requires that commercial email be identified as an advertisement and include the sender's valid physical postal address.

Each violation of the above provisions is subject to fines of up to $11,000.

## Spamming Seems to Work


If everyone ignored spam, then spamming would stop. However, because spammers find it rewarding, they keep spamming. Spam is growing, not shrinking.

## SpamCop

SpamCop is a free spam reporting service where you can report offenses to the senders' Internet Service Providers (ISPs), and sometimes their web hosts. This feedback is used to compile the "SpamCop Blocking List" (SCBL) and other lists. Those whose IP addresses are included on these lists have their mail rejected by servers that subscribe to the SCBL. Comments:

1. **Backscatter -** SpamCop is controversial in that it automatically lists IP addresses that send mail to spamtrap email addresses. Since these addresses may be falsely used as return addresses on spam messages, backscatter caused by these messages (including vacation messages and other auto-replies) can result in an otherwise innocent server being blocklisted if it fails to employ backscatter prevention techniques.

2. **Blocks Expire -** One of the unique features of the SCBL is that a listing expires automatically when no spam is reported from that source for 24 hours.

3. **Filter -** SpamCop recommends that the SCBL be used as a filter, rather than a block.

## Spammers Get Nasty with Blue Frog

Anti-spammer Blue Frog software provided a Firefox and Internet Explorer plugin allowing e-mail users to report their spam automatically, as a result, Blue Frog then sent complaints to the web sites being promoted in the spam messages – one complaint for each spam incident. In May 2006, Blue Security underwent a retaliatory DDoS attack initiated by spammers and their servers folded under the load and caused the entire hosting provider's (Six Apart) server farm to collapse. Blue Security identified the attackers as PharmaMaster – AKAs Christopher Brown, Swank, "Dollar", Joshua Burch , "zMACk", "some Russians", Leo Kuvayev, and Alex Blood. Blue Security ceased its anti-spam operation on May 16, 2006. The Spammers won.

## SPAM Blocking Solutions

Presented below is a comparison list of some of the more popular SPAM blocking utilities available today as compiled by Spam Filter Review (http://www.spamfilterreview.com/). These products range in price from $5 to $40.

Excellent
Very Good
Good
Fair
Poor

| Rank | SpamEater Pro GOLD | CA Anti-Spam SILVER | ChoiceMail One BRONZE | Spam Killer 4 | Spam Buster 5 | SpamNet 6 | Spam Agent 7 | iHateSpam 8 | MailWasher Pro 9 | SpamCatcher 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| **Reviewer Comments** | READ REVIEW | READ REVIEW | READ REVIEW | READ REVIEW | READ REVIEW | READ REVIEW | READ REVIEW | READ REVIEW | READ REVIEW | READ REVIEW |
| **Lowest Price** | BUY $24.95 | BUY $49.99 | BUY $39.95 | BUY N/A | BUY $19.95 | BUY $39.95 | BUY $29.95 | BUY $39.95 | BUY $37.00 | BUY $29.99 |
| Overall Rating | ■■■■ | ■■■□ | ■■■□ | ■■■□ | ■■■□ | ■■□□ | ■■□□ | ■■□□ | ■□□□ | ■□□□ |
| **Ratings** | | | | | | | | | | |
| Feature Set | ■■■■ | ■■□□ | ■■■□ | ■■□□ | ■■■□ | ■■□□ | ■■□□ | ■□□□ | ■□□□ | ■□□□ |
| Ease of Use | ■■■■ | ■■■□ | ■■■□ | ■■■□ | ■■□□ | ■■■□ | ■■□□ | ■■■□ | ■■■□ | ■■■□ |
| Ease of Installation | ■■■■ | ■■■□ | ■■■□ | ■■■□ | ■■■□ | ■■■□ | ■■□□ | ■■■□ | ■■■□ | ■■■□ |
| Stability | ■■■■ | ■■■■ | ■■■□ | ■■□□ | ■■■□ | ■■□□ | ■□□□ | ■□□□ | ■■□□ | ■□□□ |
| Customization | ■■■■ | ■■□□ | ■■■■ | ■■■□ | ■■■□ | ■■□□ | ■■■■ | ■■□□ | ■□□□ | ■■□□ |
| Spam Filtering | ■■■■ | ■■■□ | ■■■■ | ■■■□ | ■■■□ | ■■□□ | ■■□□ | ■■□□ | ■■□□ | ■□□□ |
| **Spam Filtering Effectiveness** | | | | | | | | | | |
| Mail NOT in Spam Folder | ■■■■ | ■■■□ | ■■■■ | ■■■□ | ■■□□ | ■■□□ | ■■□□ | ■■□□ | ■■□□ | ■■□□ |
| Spam in Spam Folder | ■■■■ | ■■■□ | ■■■□ | ■■□□ | ■■□□ | ■■□□ | ■■□□ | ■■□□ | ■■□□ | ■■□□ |
| Mail in Inbox | ■■■■ | ■■■□ | ■■■□ | ■■■□ | ■■□□ | ■■□□ | ■■□□ | ■■□□ | ■■□□ | ■■□□ |
| Spam NOT in Inbox | ■■■■ | ■■■□ | ■■■□ | ■■■□ | ■■■□ | ■■□□ | ■■□□ | ■■□□ | ■■□□ | ■■□□ |
| **Blocking Filters (Blacklist)** | | | | | | | | | | |
| Block Certain IP Addresses | ✓ | | ✓ | | ✓ | | | ✓ | ✓ | |
| Block Certain Servers | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| Block Email Addresses | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Public Blacklist Support | ✓ | | | | | ✓ | | | ✓ | ✓ |
| **Allowing Filters (Whitelist)** | | | | | | | | | | |
| Allow Specific Server | ✓ | | ✓ | | ✓ | | ✓ | ✓ | ✓ | ✓ |
| Allow Specific IP Addresses | ✓ | | ✓ | ✓ | ✓ | | | ✓ | | ✓ |
| Allow Email Addresses | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Content/Category Filters** | | | | | | | | | | |
| Pre-Set Categories | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | |
| Number of Categories | 8 | 2 | 5 | 18 | 9 | 4 | 6 | 15 | 0 | 0 |
| **Rules** | | | | | | | | | | |
| Rule Customization | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Pre-defined Rules | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ |
| Multiple Rule Selection | ✓ | | ✓ | ✓ | | ✓ | | | ✓ | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Message Handling** | | | | | | | | | | |
| Bounce | ✓ | | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ |
| Deletion Capabilities | ✓ | | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ |
| **Other Features** | | | | | | | | | | |
| Quarantine Area | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Group Collaboration | | ✓ | | | | | | | | |
| Origin Blacklist | ✓ | | | ✓ | ✓ | ✓ | | | | ✓ |
| Sensitivity Settings | ✓ | | | ✓ | ✓ | | | | | ✓ |
| Individual User Profiles | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Reporting Capabilities | | | ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ |
| View Blocked Email with Graphics On / Off | | | ✓ | ✓ | | | | ✓ | ✓ | ✓ |
| Scheduled Auto Deletion | ✓ | | ✓ | ✓ | ✓ | | | | | |
| Importing of Address Book | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | |
| Easy Upgrades Available | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Supported Environments** | | | | | | | | | | |
| POP3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Hotmail | ✓ | | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ |
| Outlook | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Outlook Express | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Eudora | ✓ | | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ |
| IMAP | | | | | ✓ | | ✓ | | ✓ | ✓ |
| AOL | | | ✓ | | | | | | ✓ | ✓ |
| Yahoo | ✓ | | ✓ | | | | | | ✓ | |
| **Customer Support** | | | | | | | | | | |
| Program Help Menu | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Product Documentation | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Technical Support Available | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| **Supported Configurations** | | | | | | | | | | |
| XP | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 2000 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 98 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 95 | | ✓ | | | | | | ✓ | ✓ | |
| NT | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| ME | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

## How Spam Blocker Programs Work

Everyday spammers find new routes to try to get into your email inbox. Most spam consists of unwanted advertising, but some can transmit viruses, adware or spyware on to your computer and cause problems. Of course, it is also extremely annoying to go to your inbox and have to look through a whole list of emails to find one legitimate email.

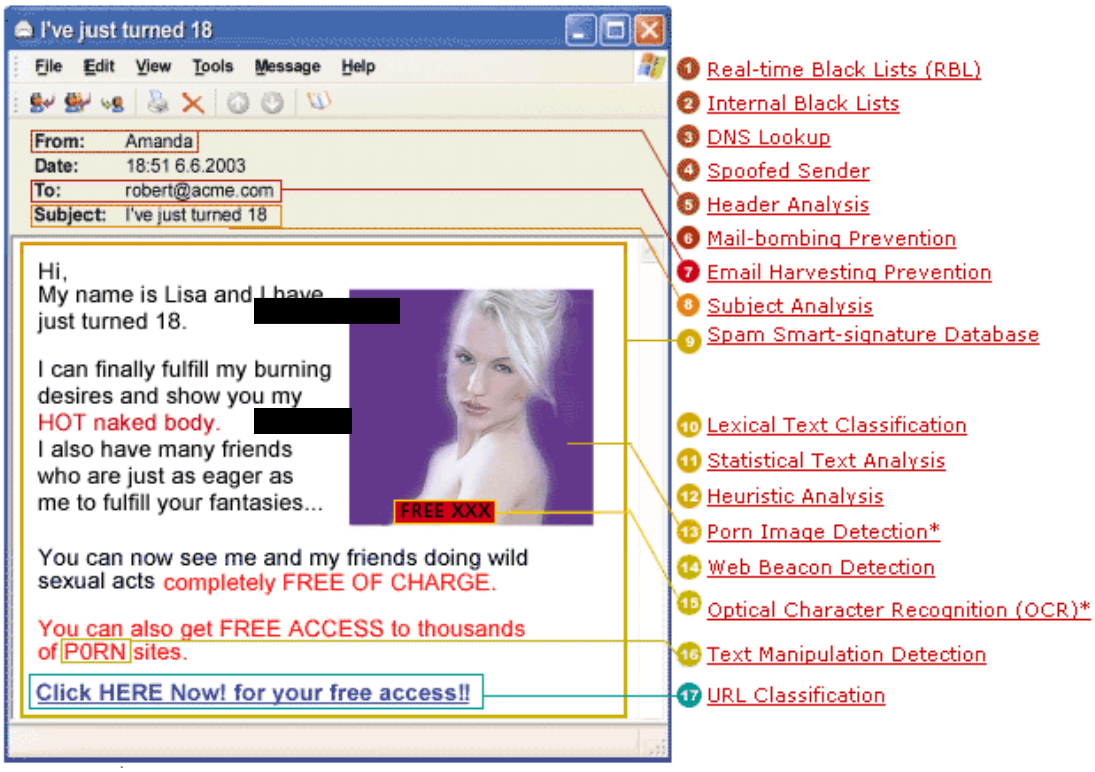
An effective anti spam program can solve many of your email problems. Not only do they block unwanted spam but they can also organize your emails into folders, so your inbox only includes wanted email. So, what does a quality spam filter do exactly? Here is a summary:

1. **Establishes White Lists and Black Lists** – A white list is a specific list of approved addresses that you set. Items not on the approved list and "known" spammers automatically go to the black list and are blocked, deleted or filed.

2. **Blocks "Sporn"** – All good programs allow you to block a high percentage of spammed pornography. Some will also filter out "adult" contented emails or block adult oriented images.

3. **Organizes Emails** – Not everyone wants to block all of their emails. Most programs will allow users to build folders, such as financial, adult oriented, games or others and the program will put incoming emails into assigned folders. This gives the user a choice about which emails they want to look at.

Presented below is a diagram highlighting the various types of information, data, and attributes today's top spam blocking systems check in order to block spam.



## Bayesian SPAM Filters

Some argue that a better approach for identifying SPAM is to employ a Bayesian filter system in which your current spam messages are statistically analyzed to create a basis for rejecting future Spam. This is important because a CPA firm will not want to use the same filtering methodology as a doctor's office that receives numerous e-mails discussing breast cancer. With Bayesian filtering, a unique and individual algorithm is created and continually updated based on the e-mails you receive and those you reject. Over time, your system learns which types of e-mails to reject automatically.

Yet, another measure you can take to block SPAM is to set up rules in your e-mail or turn on spam and adult content filtering in your e-mail client. This is discussed in more detail under e-mail tips and tricks.

## What to Look for in Spam Filter Software

Spam filters should work with your email service and offer the following features.

1. **Rules** – A good spam filtering program gives you the ability to set rules about which emails you want to receive, reject or delete.

2. **Quarantine** – Your spam filter should move mail to a quarantine folder and allow you to look through it at your own discretion.

3. **Blacklists** - You should be able to set up blacklists and whitelists.

4. **Compatible** - Most importantly – your spam filter should work with the email service that you use.

5. **Ease of Use** – The product should be easy to use even for an inexperienced computer operator.

6. **Ease of Installation & Setup** – The product should install quickly and without errors.

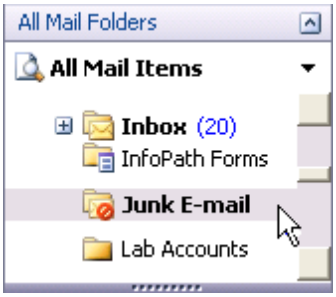
7. **Stability** – The spam filtering software should offer dependable performance and be compatible with your other programs.

8. **Block Spam** – The software should have the ability to block unwanted spam.

9. **Blocking Levels** - The software should allow the user to decide what level of filtering they want, and be in control of how the emails are organized. High filter options block and delete all emails that are not on an approved list. Lower filter levels sort all emails and save them in folders to let the user decide which ones to open or delete.

10. **Keeps Your Inbox Clean -** Your spam mail filter should go through and delete unwanted e-mail for you.

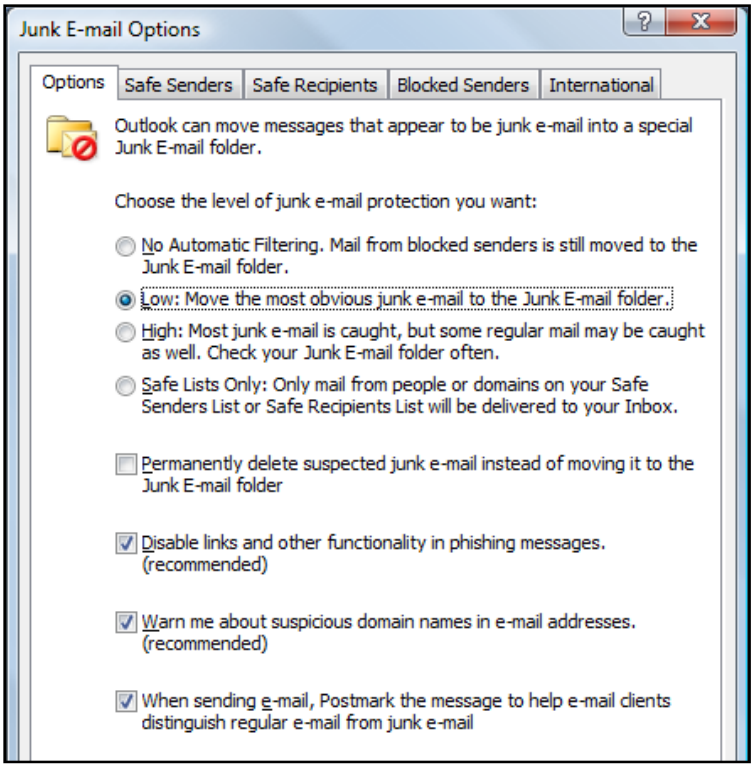
## Using Outlook's Junk E-Mail Filter




The Junk E-mail Filter in Microsoft Office Outlook 2007 is designed to catch the most obvious spam and send it to your Junk E-mail folder. The Outlook Junk E-mail Filter evaluates each incoming message based on several factors, including:

1. The time when the message was sent, and
2. The content of the message.

The filter does not single out any particular sender or message type, but instead analyzes each message based on its content and structure to discover whether or not it is probably spam. The Junk E-mail Filter is turned on by default, and the protection level is set to Low. This level is designed to catch the most obvious spam. You can make the filter more aggressive by changing the level of protection.



Also, the Junk E-mail Filter can be updated periodically to protect against the latest techniques that spammers use to spam your Inbox. Any message that is caught by the Junk E-mail Filter is moved to a special Junk E-mail folder. It is a good idea to review the messages in the Junk E-mail folder from time to time to make sure that they are not legitimate messages that you want to see. If they are legitimate, you can move them back to the Inbox by marking them as not junk. You can also drag them to any folder.

## 10 Tips to Help Reduce Spam

1. **Use the Junk E-mail Filter in Outlook** - Outlook 2007 helps to mitigate the problem of spam by providing the Junk E-mail Filter, which automatically evaluates incoming messages and sends those identified as spam to the Junk E-mail folder.

2. **Block Pictures That Spammers Use As Web Beacons** - Office Outlook 2007 has an anti-spam feature that blocks automatic picture downloads when the content is linked to a server. If you open a message that has external content when this feature is turned off, the external content downloads automatically, inadvertently verifying to the server that your e-mail address is a valid one. Your e-mail address can then be sold to a spammer. You can unblock external content for messages that come from sources that you trust.

3. **Turn Off Read And Delivery Receipts And Automatic Processing Of Meeting Requests** - Spammers sometimes resort to sending meeting requests and messages that include requests for read and delivery receipts. Responding to such meeting requests and read receipts might help spammers to verify your e-mail address. You may want to turn off this functionality.

   To turn off read receipts, on the Outlook Tools menu, click Options, E-mail Options, Tracking Options, and click Never send a response. To turn off automatically acceptance of meeting requests, Click the Outlook Tools menu, Options, Calendar Options, Advanced options, Resource Scheduling, and clear the “automatically accept meeting requests and process cancellations” check box.

4. **Protect Your E-Mail Address** - Be cautious about posting your e-mail address on public Web sites, such as newsgroups, chat rooms, bulletin boards, and so forth. When visiting public sites, you might want to use an e-mail address that is different from your main e-mail address. Remove your e-mail address from your personal Web site. Whenever you list or link to your e-mail address, you increase your chances of being spammed.

5. **Review The Privacy Policies Of Web Sites** - When you sign up for online banking, shopping, or newsletters, review the privacy policy of the site carefully before you reveal your e-mail address or other personal information. Look for a link or section (usually at the bottom of the Web site's home page) called "Privacy Statement," "Privacy Policy," "Terms and Conditions," or "Terms of Use." If the Web site does not explain how your personal information will be used, consider not using the services at that site.

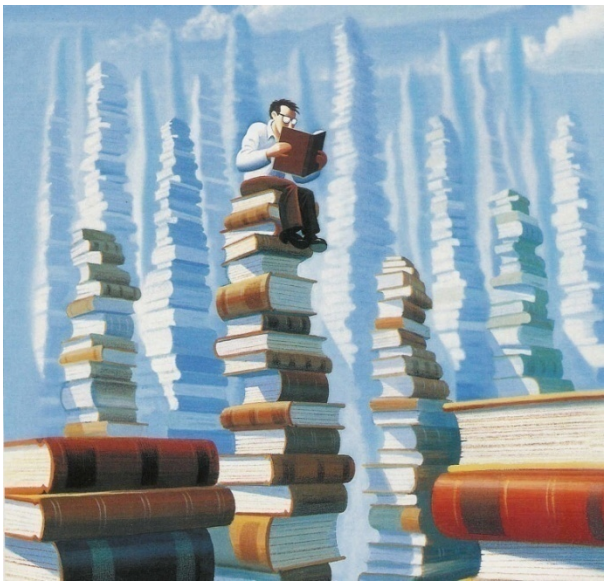
6. **Watch Out For Check Boxes That Are Already Selected** - When you shop online, companies sometimes add a check box that is already selected, which indicates that it is fine with you if the company sells or gives your e-mail address to other businesses (or "third parties"). Clear this check box so that your e-mail address is not shared.

7. **Don't Reply To Spam** - Never reply to an e-mail message — not even to unsubscribe from a mailing list — unless you know and trust the sender, such as when the e-mail message comes from a service, an online store, or newsletter that you have signed up with. Answering spam just confirms to the spammer that your e-mail address is an active one.

8. **Don’t send personal information via E-Mail** - Most legitimate companies will not ask for personal information to be sent in e-mail. Be suspicious if they do. Such a request could be a spoofed e-mail message disguised to look like a legitimate one. This tactic is known as phishing. If the possible spam appears to be sent by a company that you do business with — for example, your credit card company — then call the company to verify that they sent it, but don't use any phone number that is provided in the e-mail. Instead, use a number that you find by using other means, such as directory assistance, a statement, or a bill. If the request is a legitimate one, the company's customer service representative should be able to assist you.

9. **Don't Contribute To A Charity In Response To A Request Sent In E-Mail -** Unfortunately, some spammers prey on your goodwill. If you receive an e-mail appeal from a charity, treat it as spam. If the charity is one that you want to support, locate their telephone number or Web site to find out how you can make a contribution.

10. **Don't Forward Chain E-Mail Messages** - Besides increasing overall e-mail volume, by forwarding a chain e-mail message you might be furthering a hoax — and meanwhile, you lose control over who sees your e-mail address.

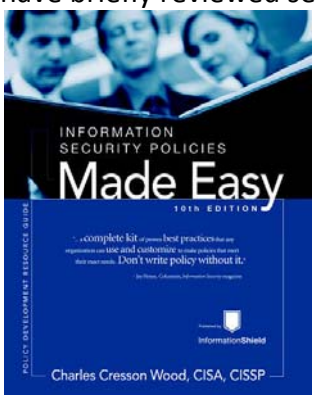


# Security Book Reviews

## Chapter 42

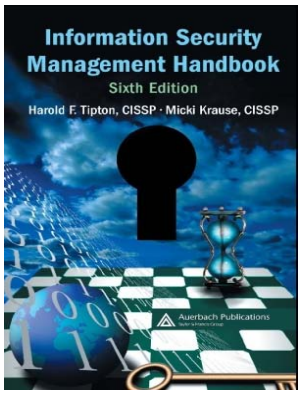
## Information Security Book Reviews

There are several dozen books available on Information Security, ranging in price from $22 to over $795. Many of these books focus on specific aspects of security such as securing network routers, protecting against identity theft, or implementing security policies. For your benefit, I have briefly reviewed several of these books for you below.



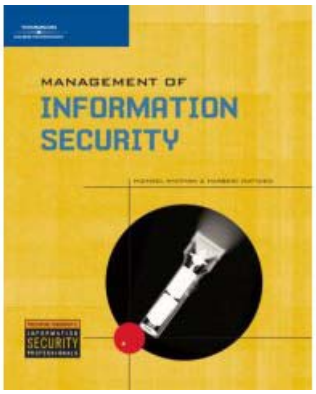

**$795** - 2005, 700+ pages + CD-ROM., by Charles Cresson Wood

This book focuses a great deal on policies and provides over 1,350 written policies and 18 policy documents including Electronic Mail Policy, Internet Security, Policy for End Users and Web Privacy Policy, High-Level Security Policy, Privacy policy, Information Ownership Policy, Firewall Policy, Data Classification Policy and Network Security Policy. If you want to CYA and inundate your people with documents and rules, this book will help you accomplish these goals.



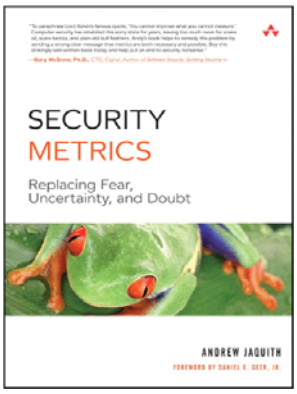

**$167 –** 2007, 3,280 pages, by Harold F. Tipson and Micki Krause

This book is a collection of dozens of articles written on a wide variety of security topics. Some articles are much better than others, and the information contained is overlapping in some areas, and missing in other areas. Selected topics included are as follows: identity management, intrusion detection, role-based networking, legislative and privacy requirements, compliance and governance, risk assessment and management, and forensics.



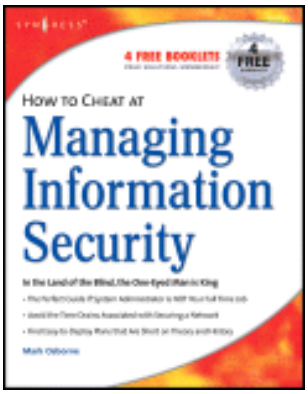

**$85 –** 2007, 600 pages, by Michael E. Whitman, and Herbert J. Mattord

This book is used more as a text in college level courses. It focuses primarily on the Common Body of Knowledge in the area of information security management as compiled by Certified Information Systems Security Professionals (CISSP).




**$31 – 2007, 400 pages, by Andrew Jaquith**

Based primarily on Yankee Group methods, the book focuses on how to establish effective metrics such as quantifying hard-to-measure security activities, compiling and analyze all relevant data, identifying strengths and weaknesses, setting cost-effective priorities for improvement, and crafting compelling messages for senior management. Also written from a CYA point of view, the book is slow to get to practical security steps in an easy to understand fashion.




**$26 – 2006, 400 pages, by Mark Osborne**

Using less-technical language, this book is written for smaller office environments, this book focuses less on policies and security governance, and more on practical measures companies can take to secure their information. It is a little easier to read and follow than the books reviewed above**.**

## Conclusion

As is the case with so many books I read, many of these books seem to take a really good lengthy article and turn it into a book that makes the reader work hard to ferret out the various tidbits of information. There are far too few checklists of action items, and far too much discussion of security theory.

# Finger Print Technology

## Chapter 43

## Fingerprint Scanners Replace Employee Time Clocks

An increasing number of businesses are using biometric scanners to log the precise time of employee arrival and departure. Some workers are doing it at Dunkin' Donuts, at Hilton hotels, even at Marine Corps bases. Employees at a growing number of businesses are starting and ending their days by pressing a hand or finger to a scanner that logs the precise time of their arrival and departure—information that is automatically reflected in payroll records. Manufacturers say these biometric devices improve efficiency and streamline payroll operations. Employers big and small buy them with the dual goals of keeping workers honest and automating outdated record-keeping systems that rely on paper time sheets. Example devices are shown below.


Cities as big as Chicago and as small as Tahlequah, Okla., have turned to fingerprint-driven ID systems to record employee work hours in recent few years. And the systems have been introduced into plenty of other workplaces without much grumbling by employees, especially those already used to punching a clock.

**Some Workers Don't Like It**

Some workers see the efforts to track their movements via fingerprints as excessive or creepy. Ricardo Hinkle, a landscape architect stated: *"Psychologically, I think it has had a huge impact on the work force here because it is demeaning and because it's a system based on mistrust"*. He called the fingerprint timekeeping systems *"a bureaucratic intrusion on professionals who never used to think twice about putting in extra time on a project they cared about, and could rely on human managers to exercise a little flexibility on matters regarding work hours".* Protests over using palm scanners to log employee time have been especially loud in New York City, where officials have spent $410 million to install an automated attendance tracking system that may eventually be used by 160,000 city workers. The city expects to save $60 million per year by modernizing a complicated record keeping system that now requires one full-time timekeeper for every 100 to 250 employees. The new system, called CityTime, would free up thousands of city employees to do less paper-pushing. Another benefit of the system is curtailing fraud. Several times each year, New York City's Department of Investigation charges city employees with taking unauthorized time off and falsifying timecards to make it looked as though they worked. Other cities have embraced similar technology.

The consulting firm International Biometric Group estimates that $635 million worth of these high-tech devices were sold last year, and projects that the industry will be worth more than $1 billion by 2011. Ingersoll Rand Security Technologies, a leading manufacturer of hand scanners based in Campbell, Calif., said it has sold at least 150,000 of the devices to Dunkin' Donuts and McDonald's franchises, Hilton hotels and to Marine Corps bases, who use them to track civilian hours.

Jon Mooney, Ingersoll Rand's general manger of biometrics, said the privacy concerns are unfounded. The hand scanners don't keep large databases of people's fingerprints—only a record of their hand shape, he said. Still, union officials in New York said they are concerned that the machines could eventually be used not just to crack down on employees skipping work, but to nitpick honest workers or invade their privacy. "The bottom line is that these palm scanners are designed to exercise more control over the workforce," said Claude Fort, president of Local 375. "They aren't there for security purposes. It has nothing to do with productivity. ... It is about control, and that is what makes us nervous."

**New Systems Prevent Time Card Fraud**

The new fingerprint time clocks prevent fraud because employees can no longer clock in or out for one another. The old trick is to sneak out of work early, asking a co-worker to punch out for you at the end of the shift - while promising to return the favor in the future. Employees who complain bitterly about the new fingerprint time clocks seem to worry most that they will no longer be able to produce fraudulent time cards.

**New Systems are Faster and Paperless**

The bottom line is that the new systems are faster and paperless, thereby saving time and reducing administration hassles. Fingerprint time clocks are now integrated with accounting systems. For example a product called “Count Me In” (costing $300 for up to 50 employees) can feed information directly to QuickBooks and other payroll and accounting programs. Rules can also be set in the system’s calendar so that an employee cannot clock in unless he is scheduled to work at that time. Neal A. Katz, a vice president at Count Me In, acknowledges that *“some workers may be skittish about providing a fingerprint”.* But he explains that his system does not store fingerprint images. Rather, it converts a fingerprint into a mathematical code based on the distance between the lines and curves on the print. *“Your fingerprint can’t be given to someone else,”* he says.

**Fingerprint Controlled Door Locks**

The BioCert® iQBio™ GuardianXL™ Fingerprint Biometric Door Lock runs exclusively on battery power. Powered by 4 AA batteries, it can be operated for up to a year without changing the batteries. Fingerprint enrollment is quick and easy. Up to 30 users can be enrolled and removed from enrollment immediately directly on the BioCert® iQBio™ GuardianXL™ Fingerprint Biometric Door Lock at the door. Benefits:


1. When someone loses their key or, worse yet, when a key is lost or stolen, regular door locks cause problems.

2. With the BioCert® iQBio™ GuardianXL™ fingerprint door lock you can program up to 138 individuals fingerprints into the lock , and then grant access to whomever you choose.
3. Walkers & Joggers don't like carry extra items like wallets, purses and keys and often the solution is to simply leave your front door open or leave a key under the mat.

4. Entrusting even the most responsible child with a key can be problematic. Keys that are lost, stolen or simply left in a desk at school will not ensure that your child arrives safely inside the house after a day at school. With a fingerprint door lock, your child can always enter their home even when you can't be there.

5. Shared Residence, Condos, Apartments & Time Shares - If you own a piece of property where you share ownership such as a condo, leased apartment or vacation home, fingerprint door lock will allow you to grant access to all ownership parties while maintaining absolute control over who has access. You can be guaranteed that there will be no key swapping or sharing and that only the authorized individuals have access using the security of Fingerprint Biometric Technology.

6. IT Rooms and Server Closets - The United States Air Force, Army and Navy are all using the BioCert® iQBio™ GuardianXL™ to secure their local IT Closets and remote server rooms.

7. Executive Suites or Executive Bathrooms - Designed around the need of small and medium business, the Guardian XL Biometric Doorlock is capable of holding 2 administrators and up to 97 additional users.

8. Human Resource Offices & Financial Records Room

9. Medical Records, Pharmacies, Regional Clinics and Doctors Offices - The Guardian XL door lock is HIPAA compliance enabled.

### Fingerprint Systems are Not Always Secure

There are ways to hack fingerprint systems.

1. Employees could be force to provide fingerprints where as password systems can utilize secondary passwords which trigger hidden alarms.

2. Fingers can be severed or chopped off; however, in March 2008 a new fingerprint reader from Futronic was released which verifies that the finger is a living finger by measuring heat, sweat and a heart beat before activating.

3. MythBusters proved that even these new readers can be fooled. They were able to recreate a latex fingerprint, install it on a live person, and lick the fingerprint to reproduce sweat. Even a photocopy of a fingerprint that was licked also beat the lock.


**Fingerprint Lock** [edit]

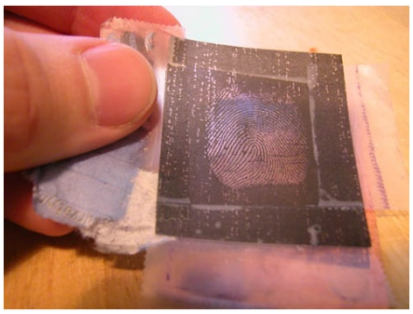
Fingerprint readers take a sample of a fingerprint and match it with an approved-person database. The particular door-mounted scanner tested optically samples the fingerprint, and also had some extra "liveness-sensing" features that supposedly looks for pulse, body heat, and sweat. The optical fingerprint reader the MythBusters installed can be fooled by...

| Myth statement | Status | Notes |
|---|---|---|
| ...a copy of an approved fingerprint etched in latex. | Confirmed | Licking the latex sample (to simulate sweat) was enough to fool the scanner. |
| ...a ballistics gel copy of an approved fingerprint. | Confirmed | Licking the gel sample (to simulate sweat) was enough to fool the scanner. |
| ...a paper copy of an approved fingerprint. | Confirmed | Licking the paper sample (to simulate sweat) was enough to fool the scanner. |

Here is the YouTube Clip: http://www.youtube.com/watch?v=LA4Xx5Noxyo

4. Fingerprints can be duplicated. One scientist in Japan was able to use a gummy bear to successfully duplicate a fingerprint.

5. Fingerprints can be reproduced. This web site walks you through the process for capturing and recreating a fingerprint: http://www.stdot.com/pub/ffs/hack3.html.



Perhaps the more common approach is to hack the fingerprint reader. On this web page two hackers explain one method for achieving this goal: http://www.securityfocus.com/news/6717.

Still another approach is to install a fake fingerprint reader which captures peoples fingerprints – in much the same way criminals use fake ATM devices to capture ATM numbers and PINs.

# Biography & Contact Information

**J. Carlton Collins, CPA - ASA Research - Carlton@ASAresearch.com - 770.734.0950**

J. Carlton Collins is an accounting software analyst and the editor of the Accounting Software Advisor web site. Since 1984, Carlton has worked in the accounting software industry installing systems, consulting with end users, lecturing to more than one hundred thousand businesses, consulting to accounting software companies, publishing books, articles and web sites. Carlton is experienced with many of the top accounting software packages such as MAS 500, BusinessWorks, Great Plains, Navision, Axapta, ACCPAC Advantage Series, Epicor, Open Systems Traverse, MAS 90, MAS 200, Exact's Macola ES, Peachtree Complete Accounting, SouthWare, SAP R/3, QuickBooks, Microsoft Office Accounting, BusinessVision 32, and more.

In 1983, Carlton developed spreadsheet templates for financial feasibility studies that were used as a basis for more than $3 billion in bond issues, including rated bonds, private placements, and junk bonds. In 1989 Carlton became an advisor to Lotus Development Corporation where he helped Lotus develop spreadsheet templates and marketing strategies. In 1992 Carlton took 2 entire days to personally demonstrate over 500 pages of suggestions for improving Microsoft Excel to the entire Excel development team – many of those features made their way into Excel 4.0, and shortly thereafter Excel became the dominate spreadsheet tool surpassing Lotus 123.

**Selected Positions, Awards & Accomplishments:**

1. 2008 Chairman of the Southeast Accounting Show - the south's largest CPA event.
2. Named “Top Ten CPA Technologists” by Accounting Technologies Magazine.
3. Named “Top 100 Most Influential CPAs ” by Accounting Technologies Magazine in multiple years.
4. Recipient of the AICPA Lifetime Technical Contribution to the CPA Profession Award.
5. 1995 Recipient of the Outstanding Discussion Leader Award from the Georgia Society of CPAs.
6. 2008 Recipient of the Outstanding Discussion Leader Award from the Alabama Society of CPAs.
7. Has personally delivered over 2,000 technology lectures around the world.
8. Has published 94+ pages of technology articles in the Journal of Accountancy.
9. Selected by Microsoft to develop 27 hour CPE training materials on Microsoft Office Accounting.
10. Lead author for PPC's Guide to Installing Microcomputer Accounting Systems.
11. Has installed accounting systems for more than 200 companies.
12. Has assisted thousands with the selection of an appropriate accounting system.
13. Past Chairperson of the AICPA Technology Conference.
14. Past Chairman of the Georgia Society of CPAs PC Advisory Committee.
15. Founder and past five-term President of the PC Consultant’s Group of Atlanta.
16. Has lectured in more than 40 States and five countries.
17. Has delivered keynote and session lectures at dozens of accounting software conferences including seven Microsoft Partner Conferences, five Sage Conferences, and multiple conferences for Epicor, Open Systems, Exact Software, Sage ACCPAC ERP, Dynamics.NAN, Dynamics.AX, SouthWare, Axapta .
18. Has provided consulting services to many computer companies *(including Compaq, IBM, Microsoft, Apple, Novell, Peachtree, Epicor, Sage Software, Softline, Exact, ACCPAC, Intuit, Peachtree, Great Plains, and others)*.

Carlton’s diverse background is an asset in providing his specialized consulting skills. He has six years of accounting, auditing and tax experience in the areas of health care, construction, distribution, automobile dealerships, insurance, manufacturing, and general business. His tax experience includes corporate, individual, partnership, fiduciary, and estate tax planning work. Carlton also has been heavily involved in the other areas of financial forecasts, bond issues, Medicare and Medicaid reimbursement, conventional financing, pension and profit sharing plans, and business planning.